同種写像暗号CSIDHのHesse曲線による構成

小濱 大輝[1]　野本 慶一郎[2,a)]　池松 泰彦[3]　縫田 光司[3,4]　小林 真一[5]

概要：本稿では，同種写像暗号の鍵共有プロトコルである CSIDH の，Hesse 曲線を用いた構成について述べる．Hesse 曲線は一般に，オリジナルな CSIDH で使用されている Montgomery 曲線と同型とは限らない．したがって我々の提案プロトコルは，新しい楕円曲線のクラスに対する鍵共有プロトコルである．

キーワード：同種写像暗号，CSIDH，Hesse 曲線

Construction of isogeny-based cryptography CSIDH by Hessian curves

Hiroki Obama[1]　Keiichiro Nomoto[2,a)]　Yasuhiko Ikematsu[3]　Koji Nuida[3,4]　Shinichi Kobayashi[5]

Abstract: In this paper, we construct CSIDH, a key-exchange protocol in isogeny-based cryptography, using Hessian curves. In general, a Hessian curve is not always isomorphic to a Montgomery curve used in the original CSIDH. Therefore, our proposed protocol is a key-exchange protocol on a new class of elliptic curves.

Keywords: Isogeny-based cryptography, CSIDH, Hessian curve

1. 導入

現在普及している暗号技術の量子計算機実現による危殆化に備え，2016 年に NIST（米国標準技術研究所）は耐量子計算機暗号の標準化に向けた公募を行なった．第一ラウンドには 69 件の暗号アルゴリズムが提案され，2022 年 7 月に始まった第四ラウンドでは 4 件の候補が残っている．残った 4 件の内の一つである SIKE [7] は，超特異楕円曲線の部分群を利用した鍵共有方式である．しかし 2022 年 7 月末に，SIKE において基盤となっている鍵共有プロトコル SIDH に対しての深刻な鍵復元攻撃 [4] が提案された．幸いなことに，その攻撃が適用できないとされている同種写像ベースの鍵共有方式に CSIDH [5] がある．

CSIDH とは，虚二次体の order $\mathcal{O}$ に付随するイデアル類群の，ある超特異楕円曲線の $\mathbb{F}_p$-同型類の集合 $\mathcal{E}\ell\ell_p(\mathcal{O})$ への作用に基づく鍵共有方式である．CSIDH では，$\mathbb{F}_p$ 上の超特異な Montgomery 曲線

$$\mathcal{M}_A : y^2 = x^3 + Ax^2 + x$$

を使用しており，素数 p に関するある条件の下，$\mathcal{E}\ell\ell_p(\mathcal{O})$ の元の代表元として一意的に Montgomery 曲線が取れるという特徴を使っている (cf. 命題 A.2.2).

Montgomery 曲線による表示を用いなくても，CSIDH の構成を行うことができる．例えば，守谷らにより Edwards 曲線と呼ばれる楕円曲線を用いて CSIDH が構成された [10]．この結果は，Edwards 曲線と Montgomery 曲線の間の 1 対 1 対応を用いている．しかし素数の条件によっては，$\mathcal{E}\ell\ell_p(\mathcal{O})$ の元で Montgomery 曲線で代表されないこともある．Montgomery 曲線を使えないときも，別の楕円曲線を用いて CSIDH が構成できるかどうか，また，どのような利点があるかを研究することは重要である．

[1] 株式会社エクサ
EXA CORPORATION
[2] 九州大学大学院数理学府
Graduate School of Mathematics, Kyushu University
[3] 九州大学マス・フォア・インダストリ研究所
Institute of Mathematics for Industry, Kyushu University
[4] 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
[5] 九州大学大学院数理学研究院
Faculty of Mathematics, Kyushu University
[a)] nomotokeiichiro@gmail.com

本論文では，Hesse 曲線と呼ばれる楕円曲線を扱う．Hesse 曲線とは，方程式

$$X^3+Y^3+Z^3=dXYZ \quad (d^3\neq 27)$$

で定義される楕円曲線であり，楕円曲線暗号においてサイドチャネル攻撃に耐性をもつモデルとして知られている [9]．Hesse 曲線は一般に，Montgomery 曲線と $\mathbb{F}_p$ 上同型とは限らない（cf. §A.1）．しかもある種の条件下では，$\mathcal{E}\ell\ell_p(\mathcal{O})$ の元の代表元として Hesse 曲線を常に取ることができる場合もある．よって，Hesse 曲線を用いて CSIDH を構成することができれば，鍵共有を行うことのできる素数 p の範囲が広がるという利点がある．

我々はこの問題に関して，位数 3 の $\mathbb{F}_p$-有理点をもつ楕円曲線は Hesse 曲線で代表されることを示し，この事実を用いて CSIDH と同様の理論を構築する．さらに，128bit 安全性のパラメータに対する実装実験を行う．

本論文の構成は以下の通りである．§2 では，Hesse 曲線に関する基本的な性質を述べる．§3 では，どのような楕円曲線が Hesse 曲線と同型になるのかということについて詳しく述べる．§4 では，Hesse 曲線へのイデアル類群の作用について説明し，実装をするために必要な作用の明示公式を与える．§5 では，実際に鍵共有のアルゴリズムを与え，実験と考察を行う．§6 では，本論文の結論を述べる．最後に付録として，§A.1 に本論文で必要となる楕円曲線に関する基本的な性質をまとめる．また，§A.2 に Hesse 曲線と Montgomery 曲線が $\mathbb{F}_p$ 上同型ではない例を与える．

2. Hesse 曲線の基本性質

ここでは，Hesse 曲線を使った鍵共有プロトコルを説明するために，Hesse 曲線の諸性質について述べる．以下では特に断らない限り，$p\geq 5$ を素数，$\mathbb{F}_q$ $(q=p^r)$ を位数 q の有限体とする．また，$\overline{\mathbb{F}_q}$ を $\mathbb{F}_q$ の代数閉包とする．

$q\equiv 2 \bmod 3$ のとき，すなわち $3\nmid \#\mathbb{F}_q^\times$ のとき，写像

$$\mathbb{F}_q\to\mathbb{F}_q,\quad x\mapsto x^3$$

は全単射である．したがってこの場合，全ての $x\in\mathbb{F}_q$ は $\mathbb{F}_q$ 内にただ一つの 3 乗根 $x^{1/3}\in\mathbb{F}_q$ をもつ．

2.1 Hesse 曲線の定義とその上の演算

ここでは，Hesse 曲線の定義を述べ，その上の演算がどのように計算できるかについて説明する．さらに，後に必要になる Hesse 曲線の位数 3 の点を記述する．

定義 2.1. $\mathbb{F}_q$ 上のツイストされた Hesse 曲線 $\mathcal{H}_{a,d}$ とは，方程式

$$aX^3+Y^3+Z^3=dXYZ \quad (a(27-d^3)\neq 0)$$

で定義され，一点 $O=[0:-1:1]\in\mathcal{H}_{a,d}$ をもつ平面射影曲線のことである．簡単のため，$\mathcal{H}_{1,d}=\mathcal{H}_d$ と書き，これを単に Hesse 曲線という．

ツイストされた Hesse 曲線における点の逆元，加法，2 倍算は例えば以下のように計算できる．詳細に関しては [1] を参考にされたい．

逆元 $P=[X(P):Y(P):Z(P)]\in\mathcal{H}_{a,d}$ に対して

$$-P=[X(P):Z(P):Y(P)].$$

加法 $P,Q\in\mathcal{H}_{a,d}$ に対して，次のように定義をする:

$$\begin{aligned}X_{P+Q}&:=X(P)^2Y(Q)Z(Q)-X(Q)^2Y(P)Z(P),\\ Y_{P+Q}&:=Z(P)^2X(Q)Y(Q)-Z(Q)^2X(P)Y(P),\\ Z_{P+Q}&:=Y(P)^2X(Q)Z(Q)-Y(Q)^2X(P)Z(P).\end{aligned}$$

このとき，$(X_{P+Q},Y_{P+Q},Z_{P+Q})\neq(0,0,0)$ ならば

$$P+Q=[X_{P+Q}:Y_{P+Q}:Z_{P+Q}].$$

2 倍算 $P=[X(P):Y(P):Z(P)]\in\mathcal{H}_{a,d}$ に対して

$$\begin{aligned}X([2]P)&=Z(P)^3X(P)-Y(P)^3X(P),\\ Y([2]P)&=Y(P)^3Z(P)-X(P)^3Z(P),\\ Z([2]P)&=X(P)^3Y(P)-Z(P)^3Y(P).\end{aligned}$$

命題 2.2 (cf. [1, Theorem 5.1])**.** $\mathbb{F}_q$ 上のツイストされた Hesse 曲線 $\mathcal{H}_{a,d}$ に対して，$a\in\mathbb{F}_q$ の 3 乗根の一つを $c\in\overline{\mathbb{F}_q}$ とおく．このとき 1 の原始 3 乗根 $\omega\in\overline{\mathbb{F}_q}$ に対して，$\mathcal{H}_{a,d}$ の位数 3 の点は以下で全てである:

$$\begin{aligned}\{&[1:0:-c],[1:-c:0],[0:-\omega:1],[0:-\omega^2:1],\\ &[1:0:-c^2],[1:-c^2:0],[0:-1:\omega],[0:-1:\omega^2]\}.\end{aligned}$$

特に $q\equiv 2 \bmod 3$ ならば

$$\mathcal{H}_d(\mathbb{F}_q)[3]=\{O,[1:0:-1],[1:-1:0]\}.$$

2.2 超特異 Hesse 曲線

ここでは，超特異な Hesse 曲線の例を与える．

命題 2.3. $p\equiv 2 \bmod 3$ ならば，$\mathcal{H}_{a,0}:aX^3+Y^3+Z^3=0$ は $\mathbb{F}_p$ 上の超特異楕円曲線である．

証明. $\#\mathcal{H}_{a,0}(\mathbb{F}_p)=p+1$ を示せばよい（cf. 注意 A.1.3）．仮定より，全ての $x\in\mathbb{F}_p$ には 3 乗根 $x^{1/3}\in\mathbb{F}_p$ が一意に存在するので，$\#\mathcal{H}_{a,0}(\mathbb{F}_p)=\#L(\mathbb{F}_p)$ である． ここで，L は射影直線 $aX+Y+Z=0$ である．また，$L\simeq\mathbb{P}^1$ であるから $\#\mathcal{H}_{a,0}(\mathbb{F}_p)=p+1$ となり，主張を得る． □

2.3 Hesse 曲線の Weierstrass 標準形

一般に，楕円曲線 E_1,E_2 の間の同型写像を具体的に記述するのは難しい．しかし E_1 と E_2 が Weierstrass 方程式で

定義されているならば，その同型写像は

$$(x,\ y) \mapsto (u^2x + r,\ u^3y + su^2x + t)$$

という形で与えられる [11, p. 59, Proposition 3.1(b)]．したがって，Hesse 曲線を Weierstrass 標準形で表しておくことは有用である．以下，$\mathbb{F}_q$ 上の楕円曲線 E_{a_1,a_3} を

$$E_{a_1,a_3} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3$$

により定義する．

命題 2.4 ([8, Remark 1])**.** $\mathbb{F}_q$ 上の楕円曲線 E_{a_1,a_3} に対して，$\delta^3 = a_1^3 - 27a_3$ となる $\delta \in \overline{\mathbb{F}_q}$ を取る．このとき $a = 1, d = 3(a_1 + 2\delta)/(a_1 - \delta)$ とおくと，変数変換

$$\begin{aligned} X' &= (2a_1 + \delta)X + 3Y + 3a_3Z, \\ Y' &= -(a_1 - \delta)X - 3Y, \\ Z' &= -(a_1 - \delta)X - 3a_3Z \end{aligned}$$

により，$\mathbb{F}_q(\delta)$ 上の同型 $\varphi_{a_1,a_3} : E_{a_1,a_3} \simeq \mathcal{H}_{a,d}$ が存在する．

注意 2.5. 特に $q \equiv 2 \bmod 3$ ならば，φ_{a_1,a_3} を $\mathbb{F}_q$ 上の同型として取ることができ，位数 3 の点 $[0:0:1] \in E_{a_1,a_3}$ は位数 3 の点 $[1:0:-1] \in \mathcal{H}_{c,d}$ に移る．

3. Hesse 曲線の特徴付け

この節では，どのような楕円曲線が Hesse 曲線で表示できるのか，また，その表示の一意性について議論する．

3.1 位数 3 の点をもつ楕円曲線

ここでは Hesse 曲線の表示に関する二つの補題を証明する．

補題 3.1. $q \equiv 2 \bmod 3$ とする．$\mathbb{F}_q$ 上の楕円曲線 E で位数 3 の点 $P \in E(\mathbb{F}_q)[3]$ をもつものを考える．このとき E は，点 $(0,0)$ を位数 3 の点としてもつ楕円曲線

$$E_\alpha : y^2 + \alpha xy + y = x^3$$

に $\mathbb{F}_q$ 上同型である． また，この同型により点 P は $(0,0) \in E_\alpha$ に移る．

証明. E の定義方程式を

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

とする． また，位数 3 の点を $P = (a,b) \in E(\mathbb{F}_q)[3]$ とする．このとき E に変数変換 $(x,y) \mapsto (x-a, y-b)$ を行うことで，E は位数 3 の点 $P = (0,0)$ をもつ楕円曲線

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$$

に $\mathbb{F}_q$ 上同型である． 今，$[2]P \neq O$ であることから $a_3 \neq 0$ が分かる．そして，変数変換 $(x,y) \mapsto (x, y + (a_4/a_3)x)$ を行い，x の項を消すことができる．したがってさらに E は

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2$$

に $\mathbb{F}_q$ 上同型である． また，$[3]P = O$ より $P = (0,0)$ における接線 $y = 0$ は三重に交わるので，$a_2 = 0$ を得る．よって，位数 3 の点 $P \in E(\mathbb{F}_q)[3]$ をもつ楕円曲線 E は

$$y^2 + a_1xy + a_3y = x^3$$

に $\mathbb{F}_q$ 上同型である．また，$a_3 \in \mathbb{F}_q^\times$ のただ一つの 3 乗根 $a_3^{1/3} \in \mathbb{F}_q^\times$ に対して変数変換

$$(x,\ y) \mapsto ((a_3^{1/3})^{-2}x,\ (a_3^{1/3})^{-3}y)$$

を行うことで，E は

$$E_\alpha : y^2 + \alpha xy + y = x^3$$

に $\mathbb{F}_q$ 上同型であることが分かる． □

補題 3.2. $q \equiv 2 \bmod 3$ とする．$\mathbb{F}_q$ 上の楕円曲線 E_α, E_β に対し，$\mathbb{F}_q$ 上の同型

$$\iota : E_\alpha \xrightarrow{\simeq} E_\beta$$

で，$(0,0) \in E_\alpha$ を $(0,0) \in E_\beta$ に移すものが存在すると仮定する．このとき ι は恒等写像であり，特に $\alpha = \beta$ である．

証明. [11, p. 59, Proposition 3.1(b)] より，同型 ι は

$$(x,\ y) \mapsto (u^2x + r,\ u^3y + su^2x + t)$$

という形の変数変換でなければならない．ただし $u \in \mathbb{F}_q^\times, r, s, t \in \mathbb{F}_q$ である．今，ι は $(0,0)$ を $(0,0)$ に移すので $r = t = 0$ を得る．したがって ι により E_β は

$$y^2 + \frac{1}{u}(\alpha + 2s)xy + \frac{1}{u^3}y = x^3 - \frac{s}{u^2}(\alpha + s)x^2 - \frac{s}{u^4}x$$

という方程式で表される． これを E_β の定義方程式の係数と比較することで $s = 0, u = 1$ を得る．よって ι は恒等写像である． □

3.2 Hesse 曲線による表示

ここでは，§3.1 で証明した二つの補題を用いて，楕円曲線が Hesse 曲線で表示できるための条件及び，その表示の一意性に関する定理を証明する．

定理 3.3. $q \equiv 2 \bmod 3$ とし，$\mathbb{F}_q$ 上の楕円曲線 E を考える．このとき，位数 3 の点 $P \in E(\mathbb{F}_q)[3]$ が存在するならば，以下が成り立つ:

(i) ある $d \in \mathbb{F}_q$ と $\mathbb{F}_q$ 上の同型 $E \to \mathcal{H}_d$ で，点 P を $[1:0:-1] \in \mathcal{H}_d$ に送るものが存在する．

(ii) (i) において，そのような d は一意的に存在する．

証明. (i) 補題 3.1 と命題 2.4 より従う．

(ii) ある $d_1, d_2 \in \mathbb{F}_q$ と，$\mathbb{F}_q$ 上の同型

$$\phi_{d_1} : E \to \mathcal{H}_{d_1}, \quad \phi_{d_2} : E \to \mathcal{H}_{d_2}$$

が存在して，$\phi_{d_1}(P) = \phi_{d_2}(P) = [1:0:-1]$ が成り立つと仮定する．また，命題 2.4 より，ある $\alpha, \beta \in \mathbb{F}_q$ と $\mathbb{F}_q$ 上の同型写像

$$\varphi_{\alpha,1} : E_{\alpha,1} \to \mathcal{H}_{d_1}, \quad \varphi_{\beta,1} : E_{\beta,1} \to \mathcal{H}_{d_2}$$

が存在して，$\varphi_{\alpha,1}((0,0)) = \varphi_{\beta,1}((0,0)) = [1:0:-1]$ が成り立つ．このとき，同型写像の合成

$$E_\alpha \xrightarrow{\varphi_{\alpha,1}} \mathcal{H}_{d_1} \xrightarrow{\phi_{d_1}^{-1}} E \xrightarrow{\phi_{d_2}} \mathcal{H}_{d_2} \xrightarrow{\varphi_{\beta,1}^{-1}} E_\beta$$

は $(0,0) \in E_\alpha$ を $(0,0) \in E_\beta$ に移すので，補題 3.2 より $\alpha = \beta$ である． したがって $d_1 = d_2$ を得る． □

定理 3.3 (i) における E が Hesse 曲線 $\mathcal{H}_{d'}$ のとき，同型写像 $\mathcal{H}_{d'} \to \mathcal{H}_d$ は，後述する Hesse 曲線における Vélu の公式（定理 4.6）を用いて計算することが可能である．

4. Hesse 曲線におけるイデアルの作用

ここでは，イデアル類群の Hesse 曲線への作用について述べる．まずオリジナルな CSIDH で用いている Montgomery 曲線への作用について述べる．$\mathcal{O}$ を虚二次体の order とする．このとき $\mathcal{E}\ell\ell_p(\mathcal{O})$ を，$\mathbb{F}_p$ 上の楕円曲線の $\mathbb{F}_p$-同型類で，$\mathbb{F}_p$ 上の自己準同型環が $\mathcal{O}$ と同型になるもの全体の集合とする．$p \equiv 3 \bmod 8$ ならば，$\mathcal{E}\ell\ell_p(\mathcal{O})$ の元の代表元として一意的に Montgomery 曲線

$$\mathcal{M}_A : y^2 = x^3 + Ax^2 + x$$

が取れる．また，$\mathcal{O}$ のイデアル類群は $\mathcal{E}\ell\ell_p(\mathcal{O})$ へ自由かつ推移的に作用することが知られている．したがってイデアル類群の作用により, Montgomery 曲線から一意的に Montgomery 曲線が構成できる．しかし $p \not\equiv 3 \bmod 8$ なる素数 p に対しては，$\mathcal{E}\ell\ell_p(\mathcal{O})$ の元の代表元として Montgomery 曲線が取れるとは限らない．したがって，CSIDH で使用できる素数 p の条件が限られてしまうという問題点がある．そこで我々は，位数 3 の $\mathbb{F}_p$-有理点をもつ楕円曲線に着目することで，イデアル類群の作用により Hesse 曲線から一意的に Hesse 曲線を構成する．その結果，$p \equiv 2 \bmod 3$ を満たす素数 p に対して鍵共有を行うことが可能になる．

4.1 楕円曲線とイデアル類群

ここではイデアル類群の定義を行う．また，イデアル類の楕円曲線への作用及び，その性質について述べる．

K を代数体, $\mathcal{O}$ を K の order とする．$\mathcal{O}$ の分数イデアル $\mathfrak{a}$ とは，0 でない K の有限生成部分 $\mathcal{O}$ 加群のことである．$\mathfrak{a}$ は，$\alpha \in K^\times$ と $\mathcal{O}$ のイデアル $\mathfrak{b}$ を用いて $\alpha\mathfrak{b}$ という表示をもつ．分数イデアルと区別するために，$\mathcal{O}$ のイデアルを整イデアルということがある．$\mathcal{O}$ の分数イデアル $\mathfrak{a}$ が可逆であるとは，ある $\mathcal{O}$ の分数イデアル $\mathfrak{b}$ が存在して $\mathfrak{ab} = \mathcal{O}$ となることをいう．このような $\mathfrak{b}$ は一意に定まり，$\mathfrak{a}^{-1}$ と書く．0 でない単項イデアル $\alpha\mathcal{O}$ ($\alpha \in K^\times$) は可逆であることに注意する．$\mathcal{O}$ の可逆な分数イデアル全体のなす群を $\mathcal{I}(\mathcal{O})$，0 でない単項イデアル全体のなす $\mathcal{I}(\mathcal{O})$ の部分群を $\mathcal{P}(\mathcal{O})$ と書く．このとき，$\mathrm{Cl}(\mathcal{O}) := \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O})$ のことをイデアル類群と呼ぶ．イデアル類群は有限アーベル群であることが知られている．また，イデアル類 $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ の代表元は，必ず整イデアルとして取ることができる．代数体の order，分数イデアル，イデアル類群に関する詳細は，例えば [6, §5, §7] を参考にされたい．

$\mathbb{F}_p$ 上の超特異楕円曲線 E に対して，Frobenius 準同型 $\pi_p : E \to E, (x,y) \mapsto (x^p, y^p)$ は $\pi_p^2 + p = 0$ を満たす．これより，虚二次体 $K = \mathbb{Q}[t]/(t^2+p)$ に対して，ある K の order $\mathcal{O}$ と，同型

$$\mathcal{O} \xrightarrow{\sim} \mathrm{End}_p(E)$$

で t を π_p に移すものが存在する．

以下では，特に断らない限り，$\mathbb{F}_p$ 上の超特異楕円曲線 E に対して "$\mathrm{End}_p(E) \simeq \mathcal{O}$" と書けば，$\mathcal{O}$ は虚二次体 $K = \mathbb{Q}[t]/(t^2+p)$ の order であり，$t \in \mathcal{O}$ を $\pi_p \in \mathrm{End}_p(E)$ に移す同型であると約束する．

定義 4.1. 部分集合 $S \subset \mathcal{O}$ に対し，各 $\alpha \in S$ を，同型 $\mathrm{End}_p(E) \simeq \mathcal{O}$ を通して，$\mathbb{F}_p$ 上の同種写像と見なす．このとき $E[S], [S]E$ を次のように定義する:

$$E[S] := \bigcap_{\alpha \in S} \mathrm{Ker}(\alpha), \quad [S]E := E/E[S].$$

$\alpha \in \mathcal{O} \setminus \{0\}$ に対して α 倍写像 $E \to E$ は $[\alpha]E \simeq E$ を誘導するので，$\mathcal{P}(\mathcal{O})$ は E に自明に作用する．したがってイデアル類 $[\mathfrak{a}]$ の E への作用 $[\mathfrak{a}]E$ が well-defined に定まる．

奇素数 ℓ を，$p+1$ を割り，$\mathcal{O}$ の判別式を割らないものとする．このとき

$$\pi_p^2 + p \equiv \pi_p^2 - 1 = (\pi_p - 1)(\pi_p + 1) \mod \ell$$

が成り立つ．したがってそのような素数 ℓ は，$\mathcal{O}$ において

$$\ell\mathcal{O} = \mathfrak{l}\bar{\mathfrak{l}} \quad (\mathfrak{l} = (\ell, t-1),\ \bar{\mathfrak{l}} = (\ell, t+1))$$

と分解する．よって $E[\mathfrak{l}] \cap E[\bar{\mathfrak{l}}] = \{O\}$ が分かる．また，$[\mathfrak{l}^{-1}] = [\bar{\mathfrak{l}}] \in \mathrm{Cl}(\mathcal{O})$ であるから，$[\mathfrak{l}^{-1}]E = [\bar{\mathfrak{l}}]E$ が成り立つ．

命題 4.2. E を $\mathbb{F}_p$ 上の超特異楕円曲線，$\mathrm{End}_p(E) \simeq \mathcal{O}$ とする．このとき可逆イデアル $\mathfrak{a}, \mathfrak{b}$ に対して次が成り立つ:

$$[\mathfrak{a}]([\mathfrak{b}]E) = [\mathfrak{b}]([\mathfrak{a}]E).$$

証明. イデアル類の作用は結合法則が成り立つことに注意する．したがって，素イデアル分解を考えることにより $[\mathfrak{l}_1]([\mathfrak{l}_2]E) = [\mathfrak{l}_2]([\mathfrak{l}_1]E)$ を示せば十分である．ただし $\mathfrak{l}_1, \mathfrak{l}_2$ は $\mathcal{O}$ の素イデアルである．$\mathfrak{l}_1 = \mathfrak{l}_2$ ならば示すことはないの

で，$\mathfrak{l}_1$ と $\mathfrak{l}_2$ は互いに素であると仮定してよい．$E' := [\mathfrak{l}_1]E$ とおき，自然な全射 $\phi_{E,\mathfrak{l}_1} : E \to E'$ を考える．このとき $\phi_{E,\mathfrak{l}_1}(E[\mathfrak{l}_2]) \subset E'[\mathfrak{l}_2]$ であるが，$E[\mathfrak{l}_1] \cap E[\mathfrak{l}_2] = \{O\}$ であるから，$\phi_{E,\mathfrak{l}_1}(E[\mathfrak{l}_2]) = E'[\mathfrak{l}_2]$ を得る．したがって

$$E'/E'[\mathfrak{l}_2] \simeq E/(E[\mathfrak{l}_1] + E[\mathfrak{l}_2])$$

が成り立つ．よって $\phi_{E',\mathfrak{l}_2} \circ \phi_{E,\mathfrak{l}_1}$ は自然な全射 $E \to E/(E[\mathfrak{l}_1] + E[\mathfrak{l}_2])$ に他ならない．同様にして $E'' := [\mathfrak{l}_2]E$ とおくことにより $\phi_{E'',\mathfrak{l}_1} \circ \phi_{E,\mathfrak{l}_2}$ は自然な全射 $E \to E/(E[\mathfrak{l}_1] + E[\mathfrak{l}_2])$ であることが分かる．したがって $\phi_{E',\mathfrak{l}_2} \circ \phi_{E,\mathfrak{l}_1} = \phi_{E'',\mathfrak{l}_1} \circ \phi_{E,\mathfrak{l}_2}$ となり，主張を得る． □

4.2 Hesse 曲線上のイデアル類の作用

$\mathcal{O}$ を $K = \mathbb{Q}[t]/(t^2 + p)$ の order とする．また，$p+1$ を割る素数 $\ell \geq 5$ を，$\mathcal{O}$ の判別式を割らないものとする．このとき $\mathcal{O}$ のイデアル $\mathfrak{l}$ を，$\mathfrak{l} = (\ell, t-1)$ とおく．さらに $\mathbb{F}_p$ 上の超特異 Hesse 曲線 $\mathcal{H}_d$ は，$\mathrm{End}_p(\mathcal{H}_d) \simeq \mathcal{O}$ を満たすとする．これらの条件の下，$\mathcal{H}_d$ 上で CSIDH を構成するために必要な $[\mathfrak{l}]\mathcal{H}_d$ と $[\bar{\mathfrak{l}}]\mathcal{H}_d$ の計算方法について説明する．

まずは $\mathcal{H}_d$ の部分群である $\mathcal{H}_d[\mathfrak{l}], \mathcal{H}_d[\bar{\mathfrak{l}}]$ が，次のように構成できることを証明する．

命題 4.3. (i) 点 $P \in \mathcal{H}_d(\mathbb{F}_p)$ は，$[(p+1)/\ell]P \neq O$ を満たすとする．このとき，$\mathcal{H}_d[\mathfrak{l}]$ は以下のように表せる:

$$\mathcal{H}_d[\mathfrak{l}] = \left\langle \left[\frac{p+1}{\ell}\right] P \right\rangle. \tag{1}$$

(ii) 点 $P \in \mathcal{H}_d(\mathbb{F}_{p^2})$ は，$\pi_p(P) = -P$ かつ，$[(p+1)/\ell]P \neq O$ を満たすとする．このとき，$\mathcal{H}_d[\bar{\mathfrak{l}}]$ は以下のように表せる:

$$\mathcal{H}_d[\bar{\mathfrak{l}}] = \left\langle \left[\frac{p+1}{\ell}\right] P \right\rangle. \tag{2}$$

証明． 式 (1) と式 (2) の両辺の位数が等しいことと

$$\mathcal{H}_d[\mathfrak{l}] = \mathcal{H}_d[\ell] \cap \mathrm{Ker}(\pi_p - 1) = \mathcal{H}_d(\mathbb{F}_p)[\ell]$$
$$\mathcal{H}_d[\bar{\mathfrak{l}}] = \mathcal{H}_d[\ell] \cap \mathrm{Ker}(\pi_p + 1)$$

であることから従う． □

よって，適切な点 $P \in \mathcal{H}_d(\mathbb{F}_p)$ を取ることによって $\mathcal{H}_d[\mathfrak{l}]$ が構成できる．また，$\mathcal{H}_d[\bar{\mathfrak{l}}]$ の構成に必要な $\pi_p(P) = -P$ となる点 $P \in \mathcal{H}_d(\mathbb{F}_{p^2})$ は以下の補題 4.4 から構成できる．そしてその構成は，アルゴリズム 1 により実装可能である．

補題 4.4. $p \equiv 3 \bmod 4$ と仮定し，$\mathbb{F}_{p^2} = \mathbb{F}_p[s]/(s^2+1)$ とする．以下の二つの条件を満たす $\alpha \in \mathbb{F}_p$ を取る．

(i) $d + 6\alpha \neq 0$.

(ii) $\beta := (2\alpha^3 - d\alpha^2 + 1)/(d + 6\alpha)$ に対して $\beta \in (\mathbb{F}_p)^2$.

このとき

$$P := [1 : \alpha + \sqrt{\beta}s : \alpha - \sqrt{\beta}s]$$

とおくと，$\pi_p(P) = -P$ を満たす．ここで，$\sqrt{\beta} \in \mathbb{F}_p$ は β の平方根の一つである．逆に，$\pi_p(P) = -P$ を満たす全ての点 $P \in \mathcal{H}_d(\mathbb{F}_{p^2})$ はこの手順で構成できる．

証明． Hesse 曲線 $\mathcal{H}_d : X^3 + Y^3 + Z^3 = dXYZ$ を X 座標に関して非斉次化することで，$\mathcal{H}_d$ のアフィンモデル

$$H_d : y^3 + z^3 + 1 = dyz \tag{3}$$

の $\mathbb{F}_{p^2}$-有理点で $(y^p, z^p) = (z, y)$ を満たす点 $(y, z) \in H_d(\mathbb{F}_{p^2})$ を構成すればよい．$y = \alpha + \alpha' s \in \mathbb{F}_{p^2}$ $(\alpha, \alpha' \in \mathbb{F}_p)$ と書くと

$$y^p = (\alpha + \alpha' s)^p = \alpha^p + \alpha'^p s^p = \alpha - \alpha' s$$

であるから，$z = \alpha - \alpha' s$ でなければならない．これより得られる関係式 $y + z = 2\alpha,\ yz = \alpha^2 + \alpha'^2$ を用いると，点 (y, z) は (3) を満たすから

$$(2\alpha)^3 - 6\alpha(\alpha^2 + \alpha'^2) + 1 = d(\alpha^2 + \alpha'^2)$$

が成り立つ．したがって

$$\alpha'^2 = \frac{2\alpha^3 - d\alpha^2 + 1}{d + 6\alpha} \tag{4}$$

を得る．以上より，$\alpha \in \mathbb{F}_p$ が与えられたときに，式 (4) の右辺が $\mathbb{F}_p$ において平方であれば，その平方根の一つを $\alpha' \in \mathbb{F}_p$ とおくことで

$$(y, z) = (\alpha + \alpha' s, \alpha - \alpha' s) \in H_d(\mathbb{F}_{p^2})$$

であり，$\pi_p((y, z)) = (z, y)$ を満たすことが分かる． □

注意 4.5. 補題 4.4 では，効率性を考えて $\mathbb{F}_{p^2}$ を $\mathbb{F}_p[s]/(s^2+1)$ により実現する．そのために実装実験を行う §5 では，$p \equiv 3 \bmod 4$ かつ $p \equiv 2 \bmod 3$ となる素数 p を取る．つまり，p は $p \equiv 11 \bmod 12$ を満たす素数である．理論上では $p \equiv 2 \bmod 3$ となる全ての素数 p に対して鍵共有を行うことができる．

アルゴリズム 1 $p \equiv 3 \bmod 4$ のとき π_p が -1 倍で作用する点 $P \in \mathcal{H}_d(\mathbb{F}_{p^2})$ の構成

Input: $d \in \mathbb{F}_p$
Output: $\pi_p(P) = -P$ を満たす点 $P \in \mathcal{H}_d(\mathbb{F}_{p^2})$

while True **:**
  $\alpha \in \mathbb{F}_p$ をランダムに取る．
  if $d + 6\alpha \neq 0$ **:**
    $\beta \leftarrow (2\alpha^3 - d\alpha^2 + 1)/(d + 6\alpha)$.
    if β が $\mathbb{F}_p$ で平方元 **:**
      $\gamma \leftarrow \sqrt{\beta}$.
      break
return $[1 : \alpha + \gamma t : \alpha - \gamma t]$

以上より，$\mathcal{H}_d[\bar{\mathfrak{l}}]$ も構成することが可能となった．ここからさらに $[\mathfrak{l}]\mathcal{H}_d, [\bar{\mathfrak{l}}]\mathcal{H}_d$ を計算するには，Vélu の公式 [12] を Hesse 曲線に適用した以下の命題を用いる．

定理 4.6 (cf. [3, Theorem 4])**.** $F = \{[s_i : t_i : 1]\}_{i=1}^{n} \cup \{O\}$ を $\mathcal{H}_d$ の有限部分群で $3 \nmid \#F = n+1$ を満たすものとする．ただし，任意の i について $s_i t_i \neq 0$ とする． このとき

$$d' := \frac{(1-2n)\lambda + 6\sum_{i=1}^{n} \frac{1}{s_i t_i}}{\prod_{i=1}^{n} s_i}$$

に対して

$$P \mapsto \left[\prod_{R \in F} X(P+R) : \prod_{R \in F} Y(P+R) : \prod_{R \in F} Z(P+R) \right]$$

は $\mathrm{Ker}\,\phi = F$ となる同種写像 $\phi : \mathcal{H}_d \to \mathcal{H}_{d'}$ を定める．

注意 4.7. (i) 定理 4.6 はツイストされた Hesse 曲線 $\mathcal{H}_{a,d}$ で証明されている [3, Theorem 4].

(ii) 定理 4.6 における同種写像 ϕ は 3 分点 $[1:0:-1] \in \mathcal{H}_d$ を $[1:0:-1] \in \mathcal{H}_{d'}$ に移すことが容易に確かめられる．

これらを踏まえると，Hesse 曲線における作用は以下のようなアルゴリズムで実装可能である．ただし，行番号 10 においてはアルゴリズム 1 を用いる．

アルゴリズム 2 Hesse 曲線における作用計算

Input: $d \in \mathbb{F}_p$，素数 $\ell \geq 5$，$e \in \mathbb{Z}$.
Output: $\mathcal{H}_{d'} = [\mathfrak{l}^e]\mathcal{H}_d$ を満たす d'.

1: **if** $e > 0$ **:**
2: **while** $e \neq 0$ **:**
3: $P \in \mathcal{H}_d(\mathbb{F}_p)$ をランダムに取る．
4: $Q \leftarrow [(p+1)/\ell]P$.
5: **if** $Q \neq O$ **:**
6: $\mathrm{Ker}\,\phi = \langle Q \rangle$ となる $\phi : \mathcal{H}_d \to \mathcal{H}_{d'}$ を計算．
7: $d \leftarrow d'$, $e \leftarrow e-1$
8: **else:**
9: **while** $e \neq 0$ **:**
10: $\pi_p(P) = -P$ となる $P \in \mathcal{H}_d(\mathbb{F}_{p^2})$ をランダムに取る．
11: $Q \leftarrow [(p+1)/\ell]P$.
12: **if** $Q \neq O$ **:**
13: $\mathrm{Ker}\,\phi = \langle Q \rangle$ となる $\phi : \mathcal{H}_d \to \mathcal{H}_{d'}$ を計算．
14: $d \leftarrow d'$, $e \leftarrow e+1$.
15: **return** d

5. Hesse 曲線を用いた鍵共有プロトコル

ここでは，Hesse 曲線を用いた CSIDH の提案手法について説明を行う．さらに，その手法の実験結果を示す．

5.1 Hesse 曲線を用いた提案手法

これまでに述べた命題を用いて，Hesse 曲線による鍵共有プロトコルを以下のように構成する．

公開鍵: $p \equiv 2 \bmod 3$ を満たす素数 p，正の整数 $n \in \mathbb{Z}$, $p+1$ を割る 5 以上の素数 $\ell_1, \cdots, \ell_n, m \in \mathbb{Z}$ 及び $\mathbb{F}_p$ 上の Hesse 曲線 $\mathcal{H}_0 : X^3 + Y^3 + Z^3 = 0$.

秘密鍵: Alice の秘密鍵 $(e_1, e_2, \ldots, e_n) \in \mathbb{Z}^n$，Bob の秘密鍵 $(d_1, d_2, \ldots, d_n) \in \mathbb{Z}^n$ を，各 i に対して e_i, d_i が区間 $[-m, m]$ に属すように一様ランダムに生成する．

鍵交換: Alice は $\mathcal{H}_A \simeq [\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}\ldots\mathfrak{l}_n^{e_n}]\mathcal{H}_0$ を計算し，通信路を通して $A \in \mathbb{F}_p$ を Bob に送る．Bob は $\mathcal{H}_B \simeq [\mathfrak{l}_1^{d_1}\mathfrak{l}_2^{d_2}\ldots\mathfrak{l}_n^{d_n}]\mathcal{H}_0$ を計算し，通信路を通して $B \in \mathbb{F}_p$ を Alice に送る．ただし，$\mathfrak{l}_i = (\ell_i, \pi_p - 1)$ である．

セッション鍵: Alice は受け取った B から $\mathcal{H}_{A'} \simeq [\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}\ldots\mathfrak{l}_n^{e_n}]\mathcal{H}_B$ を計算する．Bob は受け取った A から $\mathcal{H}_{B'} \simeq [\mathfrak{l}_1^{d_1}\mathfrak{l}_2^{d_2}\ldots\mathfrak{l}_n^{d_n}]\mathcal{H}_A$ を計算する．このとき，$S := A' = B'$ をセッション鍵として共有する．

この鍵共有の正当性は以下のようにして証明できる．まず，$p \equiv 2 \bmod 3$ となる素数 p を取っているので，命題 2.3 より $\mathcal{H}_0$ は超特異である．また，定理 4.6 と定理 3.3 より，ある $A \in \mathbb{F}_p$ が一意的に存在して $[\mathfrak{a}]\mathcal{H}_0 \simeq \mathcal{H}_A$ が成り立つ．同様にして，一意的に $[\mathfrak{b}]\mathcal{H}_0 \simeq \mathcal{H}_B$ と表示できる．Alice は通信路を通して B を受信し，$[\mathfrak{a}]\mathcal{H}_B \simeq \mathcal{H}_{A'}$ を計算する．Bob も同様に $[\mathfrak{b}]\mathcal{H}_A \simeq \mathcal{H}_{B'}$ を計算する．ここで，命題 4.2 より $\mathcal{H}_{A'} \simeq \mathcal{H}_{B'}$ であるが，この同型は $[1:0:-1]$ を $[1:0:-1]$ に移すので，定理 3.3 より $A' = B'$ を得る．

鍵交換における $\mathcal{H}_A \simeq [\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}\ldots\mathfrak{l}_n^{e_n}]\mathcal{H}_0$ の計算には，アルゴリズム 2 を繰り返し用いる．具体的には，初めに $\mathcal{H}_{A_1} \simeq [\mathfrak{l}_1^{e_1}]\mathcal{H}_0$ となる A_1 の計算を行い，その後は $\mathcal{H}_{A_i} \simeq [\mathfrak{l}_i^{e_i}]\mathcal{H}_{A_{i-1}}$ となる A_i を繰り返し計算する．よって，Hesse 曲線を用いた CSIDH はアルゴリズム 3 のように実装可能である．ただし，注意 4.5 で述べたように，行番号 3 で用いるアルゴリズム 2 は二次拡大 $\mathbb{F}_{p^2}$ の $\mathbb{F}_p[s]/(s^2+1)$ による実現に基づくものであるから，$p \equiv 2 \bmod 3$ かつ $p \equiv 3 \bmod 4$ となる素数 p を取る必要がある．すなわち素数 p は $p \equiv 11 \bmod 12$ を満たすように取る．

アルゴリズム 3 Hesse 曲線を用いた CSIDH

Input: $(e_1, e_2, \ldots, e_n) \in \mathbb{Z}^n$
Output: $[\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}\ldots\mathfrak{l}_n^{e_n}]\mathcal{H}_0 \simeq \mathcal{H}_d$ を満たす $d \in \mathbb{F}_p$

1: $d \leftarrow 0$.
2: **for all** $i = 1, 2, \ldots, n$ **:**
3: $\mathcal{H}_{d'} = [\mathfrak{l}_i^{e_i}]\mathcal{H}_d$ となる d' を計算． ▷ アルゴリズム 2
4: $d \leftarrow d'$.
5: **return** d

5.2 パラメータの選択

オリジナルな CSIDH に対する最良の攻撃法の計算量は $O(\sqrt[4]{p})$ である [5, §7.1]．したがって今回の実装実験においても，128bit 安全性に基づき，512bit で表現可能な素数を取る．具体的には，$p \equiv 11 \bmod 12$ を満たす素数

$$p = 12\ell_1\ell_2\cdots\ell_n - 1 \quad (n = 73)$$

を取る． ここで，$\ell_1, \ldots, \ell_{72}$ は 5 以上の素数を小さい順に 72 個並べたもの，$\ell_{73} = 587$ である．さらに写像

$$[-m, m]^{73} \to \mathrm{Cl}(\mathcal{O}); (e_1, \ldots, e_{73}) \mapsto [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_{73}^{e_{73}}]$$

を単射に，かつ定義域と値域の濃度が同程度となるように正の整数 $m \in \mathbb{Z}$ を定めたい．十分大きな素数 p に対して $\#\,\mathrm{Cl}(\mathcal{O}) \approx \sqrt{p}$ であることが知られているので，値域の濃度はおよそ 2^{256} である． また，定義域の濃度は $(2m+1)^{73}$ であるから，$m = 5$ と定めればよい．

オリジナルな CSIDH では素数 p のサイズを 512bit，$n = 74$ かつ $m = 5$ として実験しているため，これらのパラメータの設定は，オリジナルな CSIDH で実験されているものとほとんど同様のものであることに注意されたい．

Alice が秘密鍵から計算する値 $A \in \mathbb{F}_p$ は $\lceil \log p \rceil$bit で表現できる．したがってパラメータを表 1 のように選択した場合，$A \in \mathbb{F}_p$ のサイズは 512bit 程度となる．

表 1 Hesse 曲線を使った CSIDH の 128bit 安全性パラメータ． ここで，$\ell_1, \cdots, \ell_{72}$ は 5 以上の素数を小さい順に 72 個並べたもの，$\ell_{73} = 587$ である． $A \in \mathbb{F}_p$ は Alice が秘密鍵から作成する，Bob に送る値である．

p	$\lceil \log p \rceil$	n	m	A のサイズ
$12\ell_1\ell_2 \ldots \ell_{73} - 1$	511	5	73	512bit

5.3 実装実験と考察

実験は 16GB メモリをもつ 3.20 GHz Apple M1 チップで，Magma [2] を用いて行った．表 2 は，Alice による公開鍵からセッション鍵の生成を 1000 回行った際の実行時間の平均を表す．ここで，初期値 $\mathcal{H}_0$ から $\mathcal{H}_A$ を計算する処理を “1 回目の群作用”，Bob から受け取った B から $\mathcal{H}_{A'}$ を計算する処理を “2 回目の群作用” と表記している．

表 2 128bit 安全性パラメータに対する処理時間．（1000 回の平均を表す．）

	1 回目の群作用	2 回目の群作用
時間	3.931 ms	3.929 ms

オリジナルな CSIDH では，10000 回の鍵共有の実行平均が 40.8ms であったと報告されている [5, Table 2]．しかし我々の実装実験では，1 回目の群作用及び 2 回目の群作用はいずれも約 4 秒程かかっており，実用的であるとは言えない．したがって我々の提案プロトコルにおいて，高速化という点に関して大きく改善が必要である．

6. 結論

本論文では，Hesse 曲線を用いた鍵共有プロトコルの構成について述べた．その構成には，位数 3 の $\mathbb{F}_p$-有理点の存在性に基づく Hesse 曲線の表示の一意性が重要であった．128 ビット安全性に対する実装実験では，オリジナルな CSIDH の結果に比べて 100 倍程度の実行時間となった．したがって計算処理の大幅な高速化が求められる．

また，楕円曲線の位数 N の有理点の存在性は，モジュラー曲線 $Y_1(N)$ の有理点の存在性と深い関係がある．モジュラー曲線の理論を用いることで，Hesse 曲線以外の楕円曲線に対する CSIDH の構成を試みたい．

謝辞 本研究は，JST 次世代研究者挑戦的研究プログラム JPMJSP2136 の支援を受けたものである．

参考文献

[1] Bernstein, D. J., Chuengsatiansup, C., Kohel, D. and Lange, T.: Twisted Hessian Curves, *Progress in Cryptology – LATINCRYPT 2015* (Lauter, K. and Rodríguez-Henríquez, F., eds.), Cham, Springer International Publishing, pp. 269–294 (2015).

[2] Bosma, W., Cannon, J. and Playoust, C.: The Magma algebra system. I. The user language, *J. Symbolic Comput.*, Vol. 24, No. 3-4, pp. 235–265 (online), DOI: 10.1006/jsco.1996.0125 (1997).

[3] Broon, F. L. P., Dang, T., Fouotsa, E. and Moody, D.: Isogenies on twisted Hessian curves, *Journal of Mathematical Cryptology*, Vol. 15, No. 1, pp. 345–358 (online), DOI: doi:10.1515/jmc-2020-0037 (2021).

[4] Castryck, W. and Decru, T.: An efficient key recovery attack on SIDH (preliminary version), Cryptology ePrint Archive, Paper 2022/975 (2022).

[5] Castryck, W., Lange, T., Martindale, C., Panny, L. and Renes, J.: CSIDH: An Efficient Post-Quantum Commutative Group Action, *Advances in Cryptology – ASIACRYPT 2018* (Peyrin, T. and Galbraith, S., eds.), Cham, Springer International Publishing, pp. 395–427 (2018).

[6] Cox, D. A.: *Primes of the form $x^2 + ny^2$*, Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, second edition (2013).

[7] D Jao, R Azarderakhsh, M. C. et al.: SIKE: Supersingular isogeny key encapsulation, submission to the NIST standardization process on Post-Quantum Cryptography (2017).

[8] Farashahi, R. R. and Joye, M.: Efficient Arithmetic on Hessian Curves, *Public Key Cryptography – PKC 2010* (Nguyen, P. Q. and Pointcheval, D., eds.), Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 243–260 (2010).

[9] Joye, M. and Quisquater, J.-J.: Hessian Elliptic Curves and Side-Channel Attacks, *Cryptographic Hardware and Embedded Systems — CHES 2001* (Koç, Ç. K., Naccache, D. and Paar, C., eds.), Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 402–410 (2001).

[10] Moriya, T., Onuki, H. and Takagi, T.: How to Construct CSIDH on Edwards Curves, *Topics in Cryptology – CT-RSA 2020* (Jarecki, S., ed.), Cham, Springer International Publishing, pp. 512–537 (2020).

[11] Silverman, J. H.: *The arithmetic of elliptic curves*,

Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, New York (1986).
[12] Vélu, J.: Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A-B*, Vol. 273, pp. A238–A241 (1971).

付　　録

A.1　楕円曲線の基本性質

ここでは，楕円曲線の基本事実について述べる．詳しくは [11] を参照されたい．以下，特に断らない限り K を体とする．

定義 A.1.1. K 上の楕円曲線とは，K 上定義された種数 1 の非特異射影代数曲線 E で，一点 $O \in E(K)$ をもつ曲線のことである．ここで，$E(K)$ は E の K-有理点の集合である．

一般に，K 上の楕円曲線は適当な変換により，非特異な Weierstrass 方程式

$$\begin{aligned} &Y^2Z + a_1XYZ + a_3YZ^2 \\ &= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (a_i \in K) \end{aligned}$$

で定義される曲線に K 上同型であることが知られている．本論文で扱っている Hesse 曲線は $X^3+Y^3+Z^3 = dXYZ$ という方程式で定義されるが，これも楕円曲線であることに注意されたい．

定義 A.1.2. $\mathbb{F}_q$ 上の楕円曲線 E が超特異であるとは，$E(\overline{\mathbb{F}_p})[p] = \{O\}$ が成り立つことをいう．

注意 A.1.3. $p \geq 5$ ならば，$\mathbb{F}_p$ 上の楕円曲線 E が超特異であることと $\#E(\mathbb{F}_p) = p+1$ であることは同値である．

E, E' を K 上の楕円曲線，L/K を体の拡大とする．このとき L 上の同種写像 $\phi : E \to E'$ とは，零写像でない L 上の有理写像のことをいう．全ての L 上の同種写像 $\phi : E \to E$ と，零写像を合わせた集合を $\mathrm{End}_L(E)$ と書く．K の代数閉包 $\overline{K}$ に対し，$\mathrm{End}_{\overline{K}}(E)$ を単に $\mathrm{End}(E)$ と書く．また，楕円曲線 E が $\mathbb{F}_p$ 上で定義されているとき，$\mathrm{End}_{\mathbb{F}_p}(E)$ を $\mathrm{End}_p(E)$ と書く．

A.2　Montgomery 曲線と Hesse 曲線

ここでは超特異な Hesse 曲線 $\mathcal{H}_d : X^3+Y^3+Z^3 = dXYZ$ が，一般に Montgomery 曲線と $\mathbb{F}_p$ 上同型にならないことを示す．E を $\mathbb{F}_p$ 上の超特異楕円曲線，$\pi_p : E \to E, (x,y) \mapsto (x^p, y^p)$ を p-Frobenius 準同型とする．$\mathbb{F}_p$ 上の自己準同型環 $\mathrm{End}_p(E)$ は，対応 $\pi_p \to t$ により虚二次体 $K = \mathbb{Q}[t]/(t^2+p)$ の order に同型であった．特に

$$\mathrm{End}_p(E) = \mathbb{Z}[\pi_p] \text{ または } \mathbb{Z}[(\pi_p - 1)/2]$$

が成り立つ．$\mathrm{End}_p(E)$ が $\mathbb{Z}[\pi_p]$ と $\mathbb{Z}[(\pi_p-1)/2]$ のどちらであるかは，2 分点が全て $\mathbb{F}_p$ 有理点であるかどうかで判定ができる．

命題 A.2.1. E を $\mathbb{F}_p$ 上の超特異楕円曲線とする．このとき

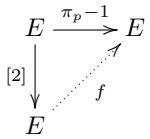
$$\mathrm{End}_p(E) = \mathbb{Z}\left[\frac{\pi_p - 1}{2}\right] \iff E[2] \subset E(\mathbb{F}_p)$$

が成り立つ．

証明．$\mathrm{End}_p(E) = \mathbb{Z}[(\pi_p-1)/2]$ と仮定する．$f := (\pi_p - 1)/2 \in \mathrm{End}_p(E)$ とおく．このとき，任意の $P \in E[2]$ に対して

$$\pi_p P - P = ([2] \circ f)(P) = (f \circ 2)(P) = O$$

であるから，$E[2]$ の点は π_p で固定される．よって $E[2] \subset E(\mathbb{F}_p)$ である．逆に $E[2] \subset E(\mathbb{F}_p)$ と仮定する．このとき任意の $P \in E[2]$ に対して $\pi_p P = P$，すなわち $E[2] \subset \mathrm{Ker}(\pi_p - 1)$ である．したがって [11, p. 73, Corollary 4.11] より $\mathbb{F}_p$ 上の同種写像 $f : E \to E$ で



が可換図式になるようなものが存在する．よって $(\pi_p - 1)/2 = f \in \mathrm{End}_p(E)$ である．　□

命題 A.2.2 ([5, p. 14, Proposition 8])**.** 5 以上の素数 p は $p \equiv 3 \bmod 8$ を満たすとする．また，$\mathbb{F}_p$ 上の楕円曲線 E は超特異であると仮定する．このとき $\mathrm{End}_p(E) = \mathbb{Z}[\pi_p]$ であることと，$A \in \mathbb{F}_p$ が存在して E と $\mathcal{M}_A : y^2 = x^3 + Ax^2 + x$ が $\mathbb{F}_p$ 上同型であることは同値である．さらに，そのような $A \in \mathbb{F}_p$ は存在すれば一意である．

命題 A.2.1 と命題 A.2.2 を用いて $\mathbb{F}_p$ 上の Hesse 曲線と Montgomery 曲線 $\mathcal{M}_A : y^2 = x^3 + Ax^2 + x$ が $\mathbb{F}_p$ 上同型でない例を挙げる．

$p = 11, d = 21$ とする．このとき直接計算することで $\mathcal{H}_d(\mathbb{F}_p) = p+1$ が分かるので，$\mathcal{H}_d$ は超特異である．したがって $\mathcal{H}_d$ と $\mathcal{M}_A$ が $\mathbb{F}_p$ 上同型でないことを示すには，命題 A.2.1 と命題 A.2.2 より，$\mathcal{H}_d[2] \subset \mathcal{H}_d(\mathbb{F}_p)$ を示せばよい．$P = [X : Y : Z] \in \mathcal{H}_d$ に対して $-P = [X : Z : Y]$ であるから，位数 2 の点は $[1 : a : a]$ という形をしていなければならない．ただし，$a \in \overline{\mathbb{F}_p}$ は $1 + 2a^3 = da^2$ を満たす．このとき $1 + 2a^3 = da^2$ の解として $a = 8, 9, 10 \in \mathbb{F}_p$ が見つかるので，$\mathcal{H}_d[2] \subset \mathcal{H}_d(\mathbb{F}_p)$ を得る．

以上より，超特異な Hesse 曲線 $\mathcal{H}_d$ は Montgomery 曲線と $\mathbb{F}_p$ 上同型になるとは限らない．