Radical Isogenies on Montgomery Curves

Hiroshi Onuki[1] and Tomoki Moriya[1]

Department of Mathematical Informatics, The University of Tokyo, Japan
{onuki,tomoki_moriya}@mist.i.u-tokyo.ac.jp

Abstract. We work on some open problems in radical isogenies. Radical isogenies are formulas to compute chains of N-isogenies for small N and proposed by Castryck, Decru, and Vercauteren in Asisacrypt 2020. These formulas do not need to generate a point of order N generating the kernel and accelerate some isogeny-based cryptosystems like CSIDH. On the other hand, since these formulas use Tate normal forms, these need to transform Tate normal forms to curves with efficient arithmetic, e.g., Montgomery curves. In this paper, we propose radical-isogeny formulas of degrees 3 and 4 on Montgomery curves. Our formulas have simple formulas to recover Montgomery coefficients and are more efficient for some cryptosystems than the original radical isogenies. In addition, we prove a conjecture left open by Castryck et al. that relates to radical isogenies of degree 4.

Keywords: Post-quantum cryptography · radical isogenies · Montgomery curves · CSIDH

1 Introduction

Recent developments in quantum computers raise the importance of research on post-quantum cryptography (PQC), which is resistant to attacks using quantum computers. Isogeny-based cryptography is one of the promising candidates for PQC. Indeed, the 3rd-round candidates in the NIST PQC competition [1] include an isogeny-based cryptosystem, SIKE [15]. An advantage of isogeny-based cryptography is that it has smaller public and private keys and ciphertext than other candidates for PQC. On the other hand, the computational costs of encryption and decryption in isogeny-based cryptography are relatively high.

The first isogeny-based cryptosystem was proposed by Couveignes [10] and by Rostovtsev and Stolbunov [20,22] independently. Their cryptosystem uses an action of the ideal class group of an order of an imaginary quadratic field on a set of ordinary elliptic curves. The action is calculated by isogenies between these elliptic curves. Isogenies between supersingular elliptic curves were brought to cryptography by Charles, Lauter, and Goren [8]. They proposed a cryptographic hash function based on supersingular isogenies. The security of their hash function is based on the hardness of path-finding in supersingular isogeny graphs. Subsequently, Jao and De Feo [16] constructed a key-exchange protocol based on the hardness of a similar problem. Their protocol, SIDH (Supersingular Isogeny Diffie-Hellman), underlies SIKE. Castryck, Lange, Martindale, Panny, and Rennes [6] proposed another key-exchange protocol using supersingular isogenies, CSIDH (commutative SIDH). As the scheme of Couveignes and Rostovtsev-Stolbunov, CSIDH uses an action of the ideal class group of an order of an imaginary quadratic field. On the other hand, CSIDH uses a set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves, and the action is calculated by isogenies defined over $\mathbb{F}_p$, where p is a large prime number. There are many protocols based on CSIDH, e.g., signature schemes, SeaSign [11] and CSI-FiSh [2]. In addition, public-key encryption schemes, SiGamal [19] and InSIDH [14], use the group action in CSIDH.

It is known that an isogeny can be computed from points in its kernel by using Vélu's formulas [24]. For accelerating the computation of isogeny-based cryptosystems, many variants of Vélu's formulas are considered. There are the formulas on Montgomery curves [13,9], Edwards curves [7,17], and Hessian curves [3]. In addition, Bernstein, De Feo, Leroux, and Smith [3] proposed a new calculation method that reduces the computational cost of the formulas from $O(\ell)$ to $\tilde{O}(\sqrt{\ell})$, where ℓ is the degree of an isogeny one compute.

Castryck, Decru, and Vercauteren [5] proposed new formulas, radical isogenies, that compute a chain of isogenies of the same degree. They showed that radical isogenies are more efficient for small degrees than other isogeny formulas. In particular, they showed that radical isogenies accelerate a variant of CSIDH.

In CSIDH, we need to compute isogenies of small degrees over $\mathbb{F}_p$ repeatedly. These isogenies correspond to the actions of ideal classes. To compute an isogeny by Vélu's formula, we need a generator of the kernel of the isogeny. We obtain the generator from a random point on the domain of the isogeny by scalar multiplication. Let E be an elliptic curve such that $(0,0)$ on E has order ℓ and φ an isogeny with kernel generated by $(0,0)$. Then a radical-isogeny formula gives the codomain E' of φ such that an isogeny with kernel generated by $(0,0)$ on E' is not the dual isogeny $\hat{\varphi}$. The coefficients of E' are expressed by an ℓ-th root of a rational expression in the coefficients of E. In CSIDH, if ℓ is odd, then there is only one ℓ-th root in $\mathbb{F}_p$. Therefore, we can determine the codomain uniquely and apply radical isogenies iteratively.

On the other hand, if ℓ is even, then there are two choices of an ℓ-th root in $\mathbb{F}_p$, i.e., x and $-x$ have the same ℓ-th power. Castryck, Decru, and Vercauteren [5] conjectured a radical-isogeny formula of degree 4 that correspond to the action of an ideal of norm 4 and left it as an open problem.

Another crucial open problem is to reduce the costs of transformations between elliptic curves in radical isogenies. Radical isogenies need to transform an elliptic curve to another curve on which the point $(0,0)$ has order ℓ. In particular, the calculation of radical isogenies are as follows:

1. Take a starting curve E as a Montgomery curve.
2. Find a point $P \in E$ of order ℓ.
3. Transform E to a curve F such that the image of P in F is $(0,0)$.
4. Apply radical isogenies of degree ℓ to F iteratively.
5. Transform the last codomain of the radical isogenies to a Montgomery curve.
6. Calculate isogenies of another degree.

	Degree 3		Degree 4	
	Formulas in [5]	**Our formula**	Formulas in [5]	**Our formula**
Isogeny	$\mathbf{E}+3\mathbf{M}+12\mathbf{A}$	$\mathbf{E}+6\mathbf{M}+12\mathbf{A}$	$\mathbf{E}+4\mathbf{M}+3\mathbf{A}+\mathbf{I}$	$\mathbf{E}+4\mathbf{M}+2\mathbf{A}+\mathbf{I}$
Transform from Montgoery	$>\mathbf{E}$	None	$2\mathbf{A}+\mathbf{I}$	$3\mathbf{A}$
Transform to Montgoery	$>3\mathbf{E}$	$3\mathbf{M}+9\mathbf{A}+\mathbf{I}$	$2\mathbf{A}+\mathbf{I}$	$\mathbf{M}+3\mathbf{A}$

Table 1. The costs of radical isogenies. The letters **E**, **M**, **A**, and **I** denote exponentiation, multiplication, addition, and inversion on $\mathbb{F}_p$, respectively.

The reason to use Montgomery curves is that Montgomery curves have efficient point addition formulas. Furthermore, if the degree ℓ is large, then the formulas on Montgomery curves is more efficient than radical isogenies. The computational costs of the transformations between Montgomery curves and curves used in radical isogenies are relatively high. Therefore, it is important to reduce these costs.

Contribution.

We work on some open problems in radical isogenies. In particular, we propose radical-isogeny formulas of degrees 3 and 4 on Montgomery curves and prove the conjecture on radical isogenies of degree 4. Since our formulas have an efficient method to calculate Montgomery coefficients, our formulas reduce the costs of the transformations. Table 1 summarizes the computational costs of our formulas and the formulas in [5] over $\mathbb{F}_p$.

Let E be a Montgomery curve, P a point on E of order 3 with x-coordinate t, and E' a Montgomery curve that is the codomain of an isogeny with kernel generated by P. Our formula of degree 3 gives the x-coordinate of a point of order 3 on E' by a rational expression in a cube root of t. Though the computational cost of our formula is higher than that of the original radical isogeny of degree 3, there is a simple formula to compute the Montgomery coefficient of E from t. Therefore, our formula could improve the computational cost in some cases.

For degree 4, we give a radical-isogeny formula between Montgomery coefficients. In addition, our formula can be simplified by using a *modified Montgomery coefficient*, which is defined by $4(A+2)$ or $4(-A+2)$, where A is a Montgomery coefficient. The computational cost of our formula is slightly less than that of the original radical isogeny of degree 4.

In addition, our formula of degree 4 proves the conjecture on radical isogenies of degree 4 by [5]. We obtain this result using an explicit formula to transform a Tate normal form to a Montgomery curve.

Organization.

Section 2 introduces mathematical tools and previous works we refer to in this paper. Section 3 gives new formulas over arbitrary fields. In Section 4, we attempt to obtain a simpler form of radical isogenies. In particular, we consider a pair of a curve and its ℓ-cyclic subgroup instead of a pair of a curve and an order-ℓ point on it. Section 5 applies the formulas in Section 3 to isogenies over $\mathbb{F}_p$. We compare the computational costs of our formulas and that of the original radical isogenies. In addition, we prove the conjugate on radical isogenies of degree 4. Finally, Section 6 concludes this paper.

2 Preliminaries

This section gives a summary of the mathematical background of this paper and introduces previous works. We refer the reader to Silverman [21] for Section 2.1 and Diamond and Shurman [12] for Section 2.2.

2.1 Elliptic Curves and Isogenies

Let K be a field. An *elliptic curve over* K is a smooth projective curve over K of genus one with a specified base point over K. For an elliptic curve E, we denote its specified base point by O_E. An elliptic curve E has an abelian group structure with identity O_E. For an extension field L over K, we denote the set of points on E defined over L by $E(L)$. Then $E(L)$ is a subgroup of E. For an integer n, we denote the multiplication-by-n map on an elliptic curve by $[n]$. The *n-torsion subgroup of* E is $\{P \in E \mid [n]P = O_E\}$ and denoted by $E[n]$. If the characteristic $\mathrm{char}(K)$ is coprime to n, we can define the *Tate pairing*, which is a bilinear map

$$t_n : E(K)[n] \times E(K)/nE(K) \to K^\times/(K^\times)^n,$$

where $E(K)[n]$ is the set of points defined over K in $E[n]$.

Let E and E' be elliptic curves over K. An *isogeny* $\varphi : E \to E'$ is a non-constant morphism such that $\varphi(O_E) = O_{E'}$. The isogeny φ induces an injection $\varphi^* : \overline{K}(E') \to \overline{K}(E)$ between the function fields of the curves. The *degree* of φ is the degree of the field extension $\overline{K}(E)/\varphi^*(\overline{K}(E'))$. We denote this by $\deg\varphi$. We say that φ is *separable (reps. inseparable)* if the extension $\overline{K}(E)/\varphi^*(\overline{K}(E'))$ is separable (resp. inseparable). The degree of φ is finite, and the cardinality of $\ker\varphi$ is less than or equal to $\deg\varphi$. Furthermore, if φ is separable, then we have $\#\ker\varphi = \deg\varphi$. Conversely, given a finite subgroup Ψ of E, there exists a separable isogeny with kernel Ψ. In addition, the codomain of an isogeny with kernel Ψ is unique up to isomorphism. We denote the codomain by E/Ψ. We call a separable isogeny whose kernel is an n-cyclic group an *n-isogeny.* For an isogeny $\varphi : E \to E'$, there exists the unique isogeny $\hat{\varphi} : E' \to E$ such that $\hat{\varphi} \circ \varphi$ is the multiplication-by-$\deg\varphi$ map on E. We call $\hat{\varphi}$ the *dual isogeny of* φ. We have $\deg\hat{\varphi} = \deg\varphi$ and that the dual isogeny of $\hat{\varphi}$ is φ.

2.2 Congruence Subgroups and Enhanced Elliptic Curves

Let N be a positive integer. The *principal congruence subgroup of level* N is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

where $\mathrm{SL}_2(\mathbb{Z})$ is the special linear group of degree 2 over $\mathbb{Z}$, i.e., the set of 2-by-2 matrices over $\mathbb{Z}$ having determinant 1. A *congruence subgroup of level* N is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that includes $\Gamma(N)$. We define two congruence subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

where $*$ means unspecified. We define an action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathcal{H}$ in $\mathbb{C}$ by

$$\begin{pmatrix} a & b \\ c & c \end{pmatrix} z = \frac{az+b}{cz+d}.$$

Then we define sets $Y(N) = \Gamma(N)\backslash\mathcal{H}$, $Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$, and $Y_1(N) = \Gamma_1(N)\backslash\mathcal{H}$. Furthermore, we can extend the action of $\mathrm{SL}_2(\mathbb{Z})$ to $\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, and define $X(N) = \Gamma(N)\backslash\mathcal{H}^*$, $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$, and $X_1(N) = \Gamma_1(N)\backslash\mathcal{H}^*$. The sets $X(N)$, $X_0(N)$, and $X_1(N)$ have structures of Riemann surfaces and are called *Modular curves.* The points in $Y(N)$, $Y_0(N)$, and $Y_1(N)$ correspond to enhanced elliptic curves over $\mathbb{C}$. An *enhanced elliptic curve for* $\Gamma_0(N)$ is an ordered pair (E, C), where E is an elliptic curve over $\mathbb{C}$ and C is an N-cyclic subgroup of E. Two enhanced elliptic curves (E, C) and (E', C') for $\Gamma_0(N)$ are *equivalent* if there exists an isomorphism $E \to E'$ that takes C to C'. We write this as $(E, C) \sim (E', C')$. The set of equivalence classes is denoted by

$$S_0(N) = \{\text{enhanced elliptic curves for } \Gamma_0(N)\}/\sim.$$

The equivalence class of an enhanced elliptic curve (E, C) is denoted by $[E, C]$. We define an enhanced elliptic curve for $\Gamma_1(N)$ as a pair of an elliptic curve over $\mathbb{C}$ and a point of order N on the curve, and an enhanced elliptic curve for $\Gamma(N)$ as a pair of an elliptic curve over $\mathbb{C}$ and an ordered pair of points that generates the N-torsion subgroup of the curve. Sets $S_1(N)$ and $S(N)$ are defined similarly to $S_0(N)$. Then there are one-to-one correspondences

$$Y_0(N) \leftrightarrow S_0(N),\ Y_1(N) \leftrightarrow S_1(N), \text{ and } Y(N) \leftrightarrow S(N).$$

In these correspondences, the natural projections in residues correspond to the natural projection in enhanced elliptic curves. For example, consider the natural projection $Y_0(p) \to Y(1)$ for a prime p. This projection corresponds to omitting the p-cyclic subgroup from an enhanced elliptic curve. Here, the index $[\Gamma(1) : \Gamma_0(p)] = p + 1$ corresponds to the number of p-cyclic subgroups of an elliptic curve.

For an arbitrary algebraically closed field, we can define enhanced elliptic curves and the sets $S_0(N)$, $S_1(N)$, and $S(N)$ in the same way. We use the same notations for these as over $\mathbb{C}$.

2.3 Montgomery Curves

We give the definition and basic properties of Montgomery curves [18]. In this subsection, we let K be a field with $\mathrm{char}(K) \neq 2$.

A *Montgomery curve over* K is an elliptic curve E defined by $y^2 = x^3 + Ax^2 + x$, where $A \in K$ such that $A^2 \neq 4$. We call A the *Montgomery coefficient* of E. We denote a point of x-coordinate $a \in K$ on a Montgomery curve by $(a, -)$. The j-invariant of E is

$$256 \frac{(A^2-3)^3}{A^2-4}.$$

This formula means that there are exactly six isomorphic Montgomery curves over $\overline{K}$ (counted with multiplicity). The number six comes from the index $[\Gamma_0(1) : \Gamma_0(4)]$. I.e., a Montgomery curve represents a class in $S_0(4)$. To explain this fact, we define a specified 4-cyclic subgroup of a Montgomery curve. By the arithmetic in Montgomery curves (see [18]), we obtain that the point $(0,0)$ on a Montgomery curve has order 2, and the x-coordinates of its halves are 1 and -1. For a Montgomery curve E, we denote the cyclic subgroup of E generated by $(1,-) \in E$ by $C_E^{(4)}$. Then we have the following.

Proposition 1. *Let E and E' be two Montgomery curves over K of Montgomery coefficients A and A', respectively. Then $(E, C_E^{(4)}) \sim (E', C_{E'}^{(4)})$ if and only if $A = A'$. Furthermore, we have $(E, \langle (0,0) \rangle) \sim (E', \langle (0,0) \rangle)$ if and only if $A^2 = A'^2$.*

Proof. From Proposition III.3.1 in [21], every isomorphism between Montgomery curves is of the form $(x,y) \mapsto (u^2x + r, u^3y)$, where $r \in \overline{K}$ and $u \in \overline{K}^{\times}$.

Let $\iota : E \to E'$ be an isomorphism that preserves $(0,0)$. Then we have $\iota(x,y) = (u^2x, u^3y)$, where $u \in \overline{K}$ such that $u^4 = 1$, and $A' = u^2A$. Therefore, we conclude $A' = \pm A$, i.e., $A^2 = A'^2$. In addition, if ι takes $C_E^{(4)}$ to $C_{E'}^{(4)}$, then $\iota((1,-)) = (1,-)$ thus $u^2 = 1$. This means $A = A'$.

Conversely, we assume $A' = -A$. Then there exists an isomorphism $\iota : E \to E'$, $(x,y) \mapsto (-x, iy)$, where i is a square root of -1 in $\overline{K}$. Since $\iota((0,0)) = (0,0)$, we have $(E, \langle (0,0) \rangle) \sim (E', \langle (0,0) \rangle)$. □

It is easy to verify that for an enhanced elliptic curve (E, C) over $\overline{K}$ for $\Gamma_0(4)$, there exist a Montgomery curve E' and an isomorphism $E \to E'$ that takes C to $C_{E'}^{(4)}$. Therefore, we can define a bijection $A : S_0(4) \to \overline{K} \backslash \{\pm 2\}$ by sending $[E, C]$ to the Montgomery coefficient of a Montgomery curve in the class $[E, C]$. The following corollary summarizes our discussion.

Corollary 2. *We have the following commutative diagram*

$$\begin{tikzcd}
S_0(4) \arrow[r] \arrow[d, "A"'] & S_0(2) \arrow[r] \arrow[d, "A^2"'] & S_0(1) \arrow[d, "j"'] \\
\overline{K}\backslash\{\pm 2\} \arrow[r] & \overline{K}\backslash\{4\} \arrow[r] & \overline{K},
\end{tikzcd}$$

where the top arrows are the natural projections, and the bottom arrows are defined by

$$A \mapsto A^2 \text{ and } a \mapsto 256\frac{(a-3)^3}{a-4}.$$

2.4 Vélu's Formulas

Vélu [24] gave explicit formulas for isogenies between elliptic curves represented as Weierstrass forms. Vélu's formulas take an elliptic curve E and a finite subgroup C of E as input and output an elliptic curve E' and a separable isogeny $\varphi : E \to E'$ with kernel C. We display some of the variants of Vélu's formulas that we need later.

Proposition 3 (Theorem 1 in [9]). *Let K be a field with $\operatorname{char}(K) \neq 2$, E a Montgomery curve over K of coefficient A, and P a point on E of order $\ell = 2d+1$. We write the x-coordinate of $[i]P$ for $i = 1, \dots, d$ as x_i. Then the Montgomery curve $y^2 = x^3 + A'x^2 + x$ with*

$$A' = \left(6\sum_{i=1}^{d}\left(\frac{1}{x_i} - x_i\right) + A\right)\left(\prod_{i=1}^{d} x_i\right)^2 \tag{1}$$

is the codomain of a separable isogeny φ with kernel $\langle P \rangle$, which is defined by

$$\varphi : (x, y) \mapsto (f(x), yf'(x)\prod_{i=1}^{d} x_i), \tag{2}$$

where

$$f(x) = x\prod_{i=1}^{d}\left(\frac{xx_i - 1}{x - x_i}\right)^2, \tag{3}$$

and $f'(x)$ is its derivative.

Note that φ in Proposition 3 sends $(1, -)$ on E to $(1, -)$ on the codomain. As we showed in Section 2.3, the coefficient A' is unique as far as we take an isogeny with this property.

For an isogeny whose kernel includes the point $(0, 0)$, we need to choose a Montgomery coefficient of its codomain. Jao and De Feo [13] gave a formula for 2-isogenies that send $(1, -)$ to $(0, 0)$.

Proposition 4 ([13]). *Let K be a field with* $\mathrm{char}(K) \neq 2$ *and E a Montgomery curve over K of coefficient A. Then the Montgomery curve $y^2 = x^3 + A'x^2 + x$ with*

$$A' = \frac{A+6}{2\alpha}, \tag{4}$$

where α is a square root of $A+2$, is the codomain of a 2-isogeny φ that sends $(1,-)$ to $(0,0)$, which is defined by

$$\varphi : (x,y) \mapsto (\frac{(x-1)^2}{2\alpha x}, \frac{1}{\beta^3} y \left(1 - \frac{1}{x^2}\right)), \tag{5}$$

where β is a square root of 2α.

Note that there are two choices of a Montgomery coefficient of the codomain, which corresponds to the sign of the square root α. The sign of the square root β is not essential since the change of the sign corresponds to the composition with the multiplication by -1.

2.5 Radical Isogenies

Let N be a positive integer, K a field with $\mathrm{char}(K) \nmid N$, E an elliptic curve over K, and P a point in $E(K)$ of order N. Then there exists an isogeny $\varphi : E \to E/\langle P \rangle$ with kernel $\langle P \rangle$. We can choose a model of $E/\langle P \rangle$ to be defined over K. Let E' be such a model. Let P' be a point on E' such that $\hat{\varphi}(P') = P$. Castryck, Decru, and Vercauteren [5] showed that P' is defined over $K(\sqrt[N]{\rho})$, where ρ is a representative of the Tate pairing $t_N(P, -P)$. The N choices of an N-th root of ρ correspond to N-isogenies different from $\hat{\varphi}$. By taking a models of E and $E/\langle P \rangle$ such that P and P' are $(0,0)$, they gave explicit formulas to compute $E/\langle P \rangle$ from E, and called these *radical isogenies*. A radical isogeny can be seen as a map on $S_1(N)$; $(E,(0,0)) \mapsto (E/\langle(0,0)\rangle,(0,0))$. For curve models, they used Tate normal forms [23] for $N \geq 4$. We write some of their formulas that we refer to later.

***N* = 3.** We use the model $E : y^2 + a_1xy + a_3y = x^3$ and $P = (0,0)$. Then a model of $E/\langle P \rangle$ such that $P' = (0,0)$ is $E' : y^2 + a_1'xy + a_3'y = x^3$ with

$$a_1' = -6\alpha + a_1 \text{ and } a_3' = 3a_1\alpha^2 - a_1^2\alpha + 9a_3, \tag{6}$$

where α is a cube root of $-a_3$.

***N* = 4.** We use the Tate normal form $E : y^2 + xy - by = x^3 - bx^2$ and $P = (0,0)$. Then a Tate normal form of $E/\langle P \rangle$ such that $P' = (0,0)$ is $E' : y^2 + xy - b'y = x^3 - b'x^2$ with

$$b' = \frac{\alpha(4\alpha^2+1)}{(2\alpha+1)^4}, \tag{7}$$

where α is a fourth root of $-b$.

***N* = 5.** We use the Tate normal form $E : y^2 + (1-b)xy - by = x^3 - bx^2$ and $P = (0,0)$. Then a Tate normal form of $E/\langle P \rangle$ such that $P' = (0,0)$ is $E' : y^2 + (1-b')xy - b'y = x^3 - b'x^2$ with

$$b' = \alpha \frac{\alpha^4 + 3\alpha^3 + 4\alpha^2 + 2\alpha + 1}{\alpha^4 - 2\alpha^3 + 4\alpha^2 - 3\alpha + 1}, \tag{8}$$

where α is a fifth root of b.

3 Radical-Isogeny Formulas on Montgomery Curves

In this section, we introduce radical-isogeny formulas of degrees 3 and 4 on Montgomery curves. In addition, we give some consideration for that of degree ≥ 5.

3.1 Degree 3.

Let K be a field with $\mathrm{char}(K) \neq 2, 3$.

As we showed in Section 2.2, a Montgomery coefficient represents a class in $S_0(4)$. A 3-cyclic subgroup of a Montgomery curve is represented by the x-coordinate of its generator. Therefore, a class in $S_0(12)$ can be represented by a pair of a Montgomery coefficient and the x-coordinate of a point of order 3. However, the genus of $X_0(12)$ is zero, so a class in $S_0(12)$ can be parametrized by one variable. Indeed, we show that the x-coordinate of a point of order 3 determines the Montgomery coefficient of the curve on which the point is.

From the arithmetic in Montgomery curves, we obtain the 3rd division polynomial of the Montgomery curve with coefficient $A \in K$:

$$x^4 + \frac{4}{3}Ax^3 + 2x^2 - \frac{1}{3}.$$

Let t be the x-coordinate of a point of order 3 on the Montgomery curve with coefficient A. Then we have

$$A = \frac{-3t^4 - 6t^2 + 1}{4t^3}. \tag{9}$$

From the condition that $A \neq \pm 2, \infty$, we have $t \neq 0, \pm 1, \pm \frac{1}{3}$. For $t \in \overline{K} \backslash \{0, \pm 1, \pm \frac{1}{3}\}$, we denote the Montgomery curve with coefficient defined by (9) by E_t, and the 3-cyclic subgroup of E_t generated by $(t, -)$ by $C_t^{(3)}$. The subgroup $C_{E_t}^{(4)} + C_t^{(3)} := \{P + Q \mid P \in C_{E_t}^{(4)}, Q \in C_t^{(3)}\}$ is cyclic of order 12. Then we have an analogue of Proposition 1.

Proposition 5. *The map*

$$T : \overline{K} \backslash \{0, \pm 1, \pm \frac{1}{3}\} \to S_0(12),\ \ t \mapsto [E_t, C_{E_t}^{(4)} + C_t^{(3)}]$$

is a well-defined bijection.

Proof. As we explained above, the map T is well-defined.

First, we show the surjectivity. Let (E, C) be an enhanced elliptic curve for $\Gamma_0(12)$ over $\overline{K}$. We decompose C to $C_3 + C_4$, where C_3 is cyclic of order 3 and C_4 is cyclic of order 4. From Proposition 1, there exists a Montgomery curve E' such that $(E', C_{E'}^{(4)}) \sim (E, C_4)$. Let $\iota : E \to E'$ be an isomorphism taking C_4 to $C_{E'}^{(4)}$, and t the x-coordinate of a generator of $\iota(C_3)$. Then $t \neq 0, \pm 1, \pm\frac{1}{3}$ and $E' = E_t$. Therefore we have $(E, C) \sim (E_t, C_{E_t}^{(4)} + C_t^{(3)})$.

Next, we show the injectivity. Let t and t' be elements in $\overline{K}\backslash\{0, \pm 1, \pm\frac{1}{3}\}$ such that there exists an isomorphism $\iota : E_t \to E_{t'}$ taking $C_{E_t}^{(4)} + C_t^{(3)}$ to $C_{E_{t'}}^{(4)} + C_{t'}^{(3)}$. From the proof of Proposition 1, we have $E_t = E_{t'}$ and $\iota((x, y)) = (x, y)$ or $(x, -y)$. Therefore, we conclude $t = t'$. □

As in the case of Montgomery curves, we have the following corollary.

Corollary 6. *We have the following commutative diagram*

$$\begin{tikzcd}
S_0(12) \arrow[r] \arrow[d, "T^{-1}"'] & S_0(4) \arrow[d, "A"] \\
\overline{K}\backslash\{0, \pm 1, \pm\frac{1}{3}\} \arrow[r] & \overline{K}\backslash\{\pm 2\},
\end{tikzcd}$$

where the top arrow is the natural projection, the left vertical arrow is the inverse of the map in Proposition 5, and the bottom arrow is defined by

$$t \mapsto \frac{-3t^4 - 6t^2 + 1}{4t^3}.$$

Using this parametrization of $S_0(12)$, we can derive a radical-isogeny formula of degree 3.

Theorem 7. *Let $t \in \overline{K}\backslash\{0, \pm 1, \pm\frac{1}{3}\}$, E be a Montgomery curve over $\overline{K}$, and $\varphi : E_t \to E$ an isogeny taking $C_{E_t}^{(4)}$ to $C_E^{(4)}$ with kernel $C_t^{(3)}$. Then the x-coordinate of a generator of* $\ker\hat{\varphi}$ *is $-\frac{1}{3t}$, and the x-coordinates of other points of order* 3 *on E are*

$$3t\alpha^2 + (3t^2 - 1)\alpha + 3t^3 - 2t, \tag{10}$$

where α is a cube root of $t(t^2 - 1)$.

Proof. From Proposition 3, the Montgomery coefficient of E is

$$\frac{-27t^4 + 18t^2 + 1}{4t}.$$

The 3rd division polynomial of E is decomposed as

$$(x + \frac{1}{3t})(x^3 + (-9t^3 + 6t)x^2 + 3t^2x - t). \tag{11}$$

It is easy to verify that $(-\frac{1}{3t}, -)$ on E generates the kernel of the dual isogeny $\hat{\varphi}$.

Let $P = (t, -)$ on E_t. An easy calculation shows that the y-coordinate of P is $\frac{t^2-1}{2\beta}$, where β is a square root of t. By the theory of radical isogenies (see Section 3 in [5]), a root of the latter factor in (11) has a rational expression in β and a cube root of the Tate pairing $t_3(P, -P)$. The isogeny φ is unchanged by replacing P with $-P$, i.e., β with $-\beta$. Therefore, the root should be in a radical extension of $\mathbb{Q}(t)$ of degree 3. Indeed, the Tate paring can be computed as

$$t_3(P, -P) = t(t^2 - 1) \bmod \mathbb{Q}(\beta)^{\times 3}.$$

Let α be a cube root of $t(t^2 - 1)$. Then the latter factor in (11) is decomposed to linear factors in $\mathbb{Q}(t, \alpha)$ and has a root of the form (10). This proves the theorem. □

The computational cost of this formula is worse than that of the original radical-isogeny formula (6). An advantage of this formula is that one can use the simple formula (9) to calculate the Montgomery coefficient from the representation t. In isogeny-based cryptosystems, Montgomery curves are used because of computational efficiency. Therefore, we need transformation between a Montgomery curve and a curve used in radial isogenies. In the case of the formula (6), the transformation needs calculating radicals. On the other hand, our transformation formula (9) does not need any radicals. We discuss the detail of this point in Section 5.3.

3.2 Degree 4.

Let K be a field with $\mathrm{char}(K) \neq 2$.

Since a Montgomery coefficient represents a class in $S_0(4) = S_1(4)$, it must be true that there exists a radical-isogeny formula of degree 4 between Montgomery coefficients. Indeed, we have the following.

Theorem 8. *Let E be a Montgomery curve with coefficient $A \in K$, E' a Montgomery curve, $\varphi : E \to E'$ an isogeny with kernel $C_E^{(4)}$, and ψ an isogeny from E' with kernel $\langle(0, 0)\rangle$. If the kernel of the composition $\psi \circ \varphi$ is cyclic, then the Montgomery coefficient A' of E' is*

$$\frac{(\beta + 2)^4}{4\beta(\beta^2 + 4)} - 2, \tag{12}$$

where β is a fourth root of $4(A + 2)$.

Proof. We decompose φ into the composition of two 2-isogenies $\varphi_2 \circ \varphi_1$. We can assume that φ_1 takes $(1, -)$ to $(0, 0)$. Let A'' be the Montgomery coefficient of $\varphi_1(E)$. From Proposition 4, we have

$$A'' + 2 = \frac{(\alpha + 2)^2}{2\alpha}, \tag{13}$$

where α is a square root of $A+2$. Again, from Proposition 4, The Montgomery coefficient of E' is

$$\frac{((\alpha+2)/\beta+2)^2}{2(\alpha+2)/\beta}-2, \tag{14}$$

where β is a square root of 2α, i.e., a fourth root of $4(A+2)$. We can obtain (12) by an easy calculation. □

By putting $a = 4(A+2)$ and $a' = 4(A'+2)$, we have a simpler formula

$$a' = \frac{(\beta+2)^4}{\beta(\beta^2+4)}, \tag{15}$$

where β is a fourth root of a. The computational cost of this formula is slightly less than that of the original radical-isogeny formula (7). In addition, as in degree 3, it is easy to transform our new representation a into the Montgomery coefficient.

3.3 Degree ≥ 5.

We could not generalize our method to the case that $N \geq 5$. Since the genus of $X_0(4N)$ is greater than 0 for $N \geq 5$, we cannot represent an element in $S_0(4N)$ by one parameter. Furthermore, we have $S_0(N) \neq S_1(N)$ for $N \geq 5$, unlike in the case that $N = 3$ or 4. As we discuss in the next section, we cannot obtain radical-isogeny formulas of degree N for a model of $S_0(N)$ for $N \geq 5$. Therefore, we have to work on a model of $S_1(N)$. A natural parametrization for the case that $N \geq 5$ is a pair of a Montgomery coefficient and the x-coordinate of a point of order N. However, even for the case that $N = 5$, the calculation is too complicated, and we could not derive any formula.

4 Consideration to Formulas on $S_0(N)$

As we stated in Section 2.5, radical isogenies of degree N can be seen as a map on $S_1(N)$. For example, for $N = 3$, consider two curves $E : y^2 + a_1xy + a_3y = x^3$ and $E' : y^2 + a'_1xy + a'_3y = x^3$. In these curves, the point $(0,0)$ has order 3. It is easy to verify that $(E,(0,0)) \sim (E',(0,0))$ if and only if $a_1^3/a_3 = {a'_1}^3/a'_3$. Note that $a_3, a'_3 \neq 0$ since the curves are smooth. By putting $T = a_1^3/a_3$ and $T' = {a'_1}^3/a'_3$, the formula (6) can be transformed to

$$T' = \frac{(\beta-6)^3}{-\beta^2+3\beta-9},$$

where β is a cube root of $-T$. (This formula is more costly than the formula (6) because of the inversion and the cubic calculation.)

As we stated in the previous section, we have $S_0(N) = S_1(N)$ for $N \leq 4$ since there is the isomorphism $[-1]$. For the case that $N \geq 5$, we could obtain a simpler isogeny formula on a parametrization of $S_0(N)$ than that of $S_1(N)$.

However, in general, we cannot obtain radical formulas on a parametrization of $S_0(N)$. We explain this in the following.

Consider the case that $N = 5$. Let K be a field with $\mathrm{char}(K) \neq 5$, and consider two elliptic curves over K defined by

$$\begin{aligned} E &: y^2 + (1-b)xy - by = x^3 - bx, \\ E' &: y^2 + (1-b')xy - b'y = x^3 - b'x. \end{aligned}$$

These curves are in Tate normal form, and the points $(0,0)$ on these curves have order 5. The cyclic subgroup of E generated by $(0,0)$ is

$$\{O_E, (0,0), (b,b^2), (b,0), (0,b)\}.$$

From this, it is easy to verify that $(E,(0,0)) \sim (E',(0,0))$ if and only if $b = b'$ and that $(E,\langle(0,0)\rangle) \sim (E',\langle(0,0)\rangle)$ if and only if $b = b'$ or $b = -\frac{1}{b'}$, i.e., $\frac{b^2-1}{b} = \frac{b'^2-1}{b'}$. Therefore, $\frac{b^2-1}{b}$ is a parametrization of $S_0(5)$. Note that b and $-\frac{1}{b}$ is the roots of $x^2 - \frac{b^2-1}{b}x - 1$.

Let E and E' be elliptic curves defined by the equations above. We define $\beta = \frac{b^2-1}{b}$ and $\beta' = \frac{b'^2-1}{b'}$. From the radical-isogeny formula (8), we have $\mathbb{Q}(b') = \mathbb{Q}(\sqrt[5]{b})$. In this setting, we show that $\beta' := \frac{b'^2-1}{b'}$ does not have any rational expression in a fifth root of any element in $\mathbb{Q}(\beta)$.

As we mentioned above, the field extension $\mathbb{Q}(b)/\mathbb{Q}(\beta)$ is of degree 2. Let $\zeta_5 \in \mathbb{C}$ be a primitive fifth root of unity. By adjoining ζ_5 to the field extension $\mathbb{Q}(b')/\mathbb{Q}(\beta)$, we obtain the Galois extension $\mathbb{Q}(\zeta_5)(b')/\mathbb{Q}(\zeta_5)(\beta)$ of degree 10. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_5)(b')/\mathbb{Q}(\zeta_5)(\beta))$ is generated by automorphisms $\sigma : b' \mapsto -\frac{1}{b'}$ and $\tau : b' \mapsto \zeta_5 b'$. The fixed field of σ is $\mathbb{Q}(\zeta_5)(\beta')$ and that of τ is $\mathbb{Q}(\zeta_5)(b)$. It is easy to verify that $\tau^{-1}\sigma\tau \neq \sigma$. Therefore, the group $\langle\sigma\rangle$ is not a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)(b')/\mathbb{Q}(\zeta_5)(\beta))$, i.e., the extension $\mathbb{Q}(\zeta_5)(\beta')/\mathbb{Q}(\zeta_5)(\beta)$ is not a Galois extension. This means that β' cannot be expressed as any rational expression in any element in $\mathbb{Q}(\zeta_5)(\beta)$. The diagram in Fig. 1 summarizes the discussion.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_5)(b) \arrow[r, dash, "\text{cyclic of degree 5}"] \arrow[d, dash, "\text{degree 2}"'] & \mathbb{Q}(\zeta_5)(b') \arrow[d, dash, "\text{degree 2}"] \\
\mathbb{Q}(\zeta_5)(\beta) \arrow[r, dash, "\text{not Galois}"'] & \mathbb{Q}(\zeta_5)(\beta')
\end{tikzcd}$$

Fig. 1. The tower of field extensions

To obtain a radical-isogeny formula for $S_0(N)$, we need to find a parametrization for $S_0(N)$ that makes the bottom extension in the diagram in Fig. 1 a Galois extension. We do not have any result for the existence of such parametrization. However, it seems to be complicated to find it. We leave this as an open problem.

5 Application to Cryptography

In this section, we consider the application of our formulas in Section 3 to CSIDH and its variants.

CSIDH uses the action of the ideal class group of an order of an imaginary quadratic field on supersingular elliptic curves. The action is calculated by isogenies defined over a finite prime field $\mathbb{F}_p$. Therefore, we consider formulas of such isogenies.

Let $\mathcal{O}$ be $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, and $\mathcal{E}\ell\ell_p(\mathcal{O})$ the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ whose $\mathbb{F}_p$-endomorphism ring is isomorphic to $\mathcal{O}$. Note that the p-th power Frobenius endomorphism π corresponds to $\sqrt{-p}$ or $-\sqrt{-p}$. We identify the $\mathbb{F}_p$-endomorphism ring of a curve with $\mathcal{O}$ under the former isomorphism. If $\mathcal{E}\ell\ell_p(\mathcal{O})$ is nonempty, then the ideal class group $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on $\mathcal{E}\ell\ell_p(\mathcal{O})$ (Theorem 7 in [6]). The group action is defined as follows: Let $E \in \mathcal{E}\ell\ell_p(\mathcal{O})$, and $[\mathfrak{a}]$ be an ideal class in $\mathrm{cl}(\mathcal{O})$ represented by an integral ideal $\mathfrak{a}$. Then the action of $[\mathfrak{a}]$ on E is defined by $[\mathfrak{a}] * E = E/E[\mathfrak{a}]$, where $E[\mathfrak{a}]$ is the $\mathfrak{a}$-torsion subgroup of E, which is defined by $\{P \in E \mid \alpha(P) = O_E \text{ for all } \alpha \in \mathfrak{a}\}$, and we take an isogeny with kernel $E[\mathfrak{a}]$ defined over $\mathbb{F}_p$.

We restrict our attention to the case that $p \equiv 3 \pmod 4$ since there is no supersingular Montgomery curve over $\mathbb{F}_p$ if $p \equiv 1 \pmod 4$ [4]. We fix a square root of -1 in $\mathbb{F}_{p^2}$ and denote it by i. Note that $i \notin \mathbb{F}_p$ in our case.

5.1 Degree-3 Isogenies

Assume that $3 \mid p + 1$ so that a supersingular elliptic curve over $\mathbb{F}_p$ has an $\mathbb{F}_p$-rational point of order 3. Then the map $\mathbb{F}_p \to \mathbb{F}_p; a \mapsto a^3$ is bijective. Therefore, there is only one cube root of an element of $\mathbb{F}_p$. For $a \in \mathbb{F}_p$, the cube root of a in $\mathbb{F}_p$ is computed by the exponentiation a^e, where e is an integer such that $e \equiv 3^{-1} \pmod{p-1}$.

Let E be a Montgomery curve in $\mathcal{E}\ell\ell_p(\mathcal{O})$. The role of 3-isogenies in CSIDH is to compute the actions of prime ideals $[3, \sqrt{-p} - 1]$ and $[3, \sqrt{-p} + 1]$, where we denote the ideal in $\mathcal{O}$ generated by a and b by $[a, b]$. The torsion subgroup $E[3, \sqrt{-p} - 1]$ is generated by a point P of order 3 such that $\pi(P) = P$, and $E[3, \sqrt{-p} + 1]$ is generated by a point Q of order 3 such that $\pi(Q) = -Q$. Note that the x-coordinates of P and Q are in $\mathbb{F}_p$. We can use Theorem 7 to compute the actions of these ideals.

Corollary 9. *Let E be a Montgomery curve in $\mathcal{E}\ell\ell_p(\mathcal{O})$, and t the x-coordinate of a generator of $E[3, \sqrt{-p} - 1]$ (resp. $E[3, \sqrt{-p} + 1]$). Then $[3, \sqrt{-p} - 1] * E$ (resp. $[3, \sqrt{-p} + 1] * E$) can be defined as a Montgomery curve E' over $\mathbb{F}_p$ such that the x-coordinate of a generator of $E'[3, \sqrt{-p} - 1]$ (resp. $E'[3, \sqrt{-p} + 1]$) is*

$$3t\alpha^2 + (3t^2 - 1)\alpha + 3t^3 - 2t, \tag{16}$$

where α is the cube root of $t(t^2 - 1)$ in $\mathbb{F}_p$.

Proof. We prove the case for $E[3, \sqrt{-p} - 1]$. The other case can be proved by the same way.

Let t' be an element in $\mathbb{F}_p$ defined by the equation (16), and E' a Montgomery curve that has an order-3 point with x-coordinate t'. From Theorem 7, E' is the codomain of the isogeny φ in Proposition 3 with kernel generated by $(t, -)$. Because $t \in \mathbb{F}_p$, the isogeny φ is defined over $\mathbb{F}_p$. Therefore, E' is a representative of the $\mathbb{F}_p$-isomorphism class $[3, \sqrt{-p} - 1] * E$. Because α is only one cube root of $t(t^2 - 1)$ in $\mathbb{F}_p$, the element t' is only one element such that the point $(t', -)$ on E' has order 3 and generates the kernel of an isogeny different from $\hat{\varphi}$. This means that t' is the x-coordinate of a generator of $E'[3, \sqrt{-p} - 1]$. □

A Formula for Montgomery$^-$ Curves. A *Montgomery$^-$ curve* over a field K with $\mathrm{char}(K) \neq 2$ is an elliptic curve defined by $y^2 = x^3 + Ax^2 - x$, where $A \in K$ such that $A^2 \neq -4$.

Castryck and Decru [4] introduced Montgomery$^-$ curves for a model of a variant of CSIDH they proposed, CSURF. CSURF uses Montgomery$^-$ curves since there is a one-to-one correspondence between Montgomery$^-$ coefficients and classes in $\mathcal{E}\ell\ell_p(\mathbb{Z}[\frac{1+\sqrt{-p}}{2}])$.

The arithmetic and isogeny formulas on Montgomery$^-$ curves are given in [4]. As same as Montgomery curves, the x-coordinate t of a point of order 3 on a Montgomery$^-$ curve determines the Montgomery$^-$ coefficient A. Indeed, we have

$$A = \frac{-3t^4 + 6t + 1}{4t^3}.$$

From the conditions $A^2 \neq -4$ and $A \neq \infty$, we have $t \neq 0, \pm i, \pm \frac{i}{3}$. For $t \in \mathbb{F}_p \backslash \{0\}$, we denote the Montgomery$^-$ curve with coefficient defined by (9) by E_t^-, and the order-3 cyclic subgroup of E_t^- generated by $(t, -)$ by $C_t^{(3-)}$.

The point $(0, 0)$ on Montgomery$^-$ curve has order 2, and the x-coordinates of halves of $(0, 0)$ are $\pm i$. Therefore, it is natural to use isogenies that send $(i, -)$ to $(i, -)$ between Montgomery$^-$ curves. However, if we use curves in $\mathcal{E}\ell\ell_p(\mathcal{O})$, such isogenies are not defined over $\mathbb{F}_p$ in general. A formula of isogenies over $\mathbb{F}_p$ between Montgomery$^-$ curves is given by Proposition 2 in [4]. By combining the formula in [4] and the proof of Theorem 7, we obtain the following formula for Montgomery$^-$ curves.

Theorem 10. *Let $t \in \mathbb{F}_p \backslash \{0\}$, E be a Montgomery curve$^-$ over $\mathbb{F}_p$, and $\varphi : E_t^- \to E$ an isogeny with kernel $C_t^{(3-)}$ defined over $\mathbb{F}_p$ that sends $(0, 0)$ to $(0, 0)$. Then the x-coordinate of a generator of $\ker \hat{\varphi}$ is $-\frac{1}{3t}$, and the x-coordinates of other points of order 3 on E are expressed by*

$$3t\alpha^2 + (3t^2 + 1)\alpha + 3t^3 + 2t, \tag{17}$$

where α is a cube root of $t(t^2 + 1)$.

By choosing α in $\mathbb{F}_p$, we can obtain a similar result to Corollary 9.

5.2 Degree-4 Isogenies

We consider the case that $p \equiv 7 \pmod 8$ and $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, which is the setting in CSURF. In this case, the prime 2 splits as the product of $[2, \frac{1-\sqrt{-p}}{2}]$ and $[2, \frac{1+\sqrt{-p}}{2}]$ in $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. As in [4], for $a \in (\mathbb{F}_p^\times)^2$, we denote the square root of a that is a square in $\mathbb{F}_p$ by $\sqrt{a}$ and define $\sqrt[4]{a} := \sqrt{\sqrt{a}}$. Note that $\sqrt{a}$ can be computed by $a^{\frac{p+1}{4}}$, and $\sqrt[4]{a}$ by $a^{\frac{p+1}{8}}$.

Our purpose is to apply Theorem 8 to computing the actions of the squares of the prime ideals above 2. Unlike the case of degree 3, the squaring map in $\mathbb{F}_p$ is not bijective. Therefore, we need to determine a square root (or a fourth root) that corresponds to the action of an ideal class we want to compute.

As considered in [4], every class in $\mathcal{E\ell\ell}_p(\mathbb{Z}[\frac{1+\sqrt{-p}}{2}])$ contains exactly two Montgomery curve over $\mathbb{F}_p$. In one of them, the point $(0,0)$ generates the $[2, \frac{1-\sqrt{-p}}{2}]$-torsion subgroup, and in the other curve, the point $(0,0)$ generates the $[2, \frac{1+\sqrt{-p}}{2}]$-torsion subgroup.

In the following, we let E be a Montgomery curve over $\mathbb{F}_p$ in $\mathcal{E\ell\ell}_p(\mathbb{Z}[\frac{1+\sqrt{-p}}{2}])$, and A the Montgomery coefficient of E. First, we show how to determine which ideal the point $(0,0)$ generates.

Lemma 11. *The point* $(0,0)$ *on* E *generates* $E[2, \frac{1-\sqrt{-p}}{2}]$ *if and only if* $A+2 \in (\mathbb{F}_p^\times)^2$ *and* $E[2, \frac{1+\sqrt{-p}}{2}]$ *if and only if* $-A+2 \in (\mathbb{F}_p^\times)^2$

Proof. From Lemma 5 in [4], the point $(0,0)$ generates $E[2, \frac{1-\sqrt{-p}}{2}]$ if and only if $(0,0)$ has a half in $E(\mathbb{F}_p)$. Furthermore, if $(0,0)$ has a half in $E(\mathbb{F}_p)$, then its all halves are in $E(\mathbb{F}_p)$ since $E \in \mathcal{E\ell\ell}_p(\mathbb{Z}[\frac{1+\sqrt{-p}}{2}])$ implies $E[2] \subset E(\mathbb{F}_p)$.

Let $P = (1, -)$ on E. Then P is a half of $(0,0)$, and the y-coordinate of P is a square root of $A+2$. Therefore, P has a half in $E(\mathbb{F}_p)$ if and only if $A+2 \in (\mathbb{F}_p^\times)^2$.

Because $E[2] \subset E(\mathbb{F}_p)$, the all roots of $x^3 + Ax^2 + x$ are in $\mathbb{F}_p$. This means that $A^2 - 4 \in (\mathbb{F}_p^\times)^2$. Therefore, if $A+2 \notin (\mathbb{F}_p^\times)^2$, then $-A+2 \in (\mathbb{F}_p^\times)^2$. This proves the latter of the lemma. □

We define the *modified Montgomery coefficient* a *of* E as $a = 4(A+2)$ if $A+2 \in (\mathbb{F}_p^\times)^2$ and $a = 4(-A+2)$ if $-A+2 \in (\mathbb{F}_p^\times)^2$. Note that a is always in $(\mathbb{F}_p^\times)^2$. To simplify notation, we let $\mathfrak{a} = [2, \frac{1-\sqrt{-p}}{2}]$ if $A+2 \in (\mathbb{F}_p^\times)^2$ and $\mathfrak{a} = [2, \frac{1+\sqrt{-p}}{2}]$ if $-A+2 \in (\mathbb{F}_p^\times)^2$. Then we can compute the action of $\mathfrak{a}$ as follows.

Lemma 12. *Let* E' *be a representative of the* $\mathbb{F}_p$*-isomorphism class* $\mathfrak{a} * E$ *that is expressed as the Montgomery curve over* $\mathbb{F}_p$ *such that* $(0,0)$ *on* E' *generates* $E'[\mathfrak{a}]$. *Then the modified Montgomery coefficient of* E' *is*

$$\frac{(\sqrt{a}+4)^2}{\sqrt{a}}. \tag{18}$$

Proof. If $A+2 \in (\mathbb{F}_p^\times)^2$, then the isogeny φ in Proposition 4 is defined over $\mathbb{F}_p$ by taking $\alpha = \sqrt{A+2}$. Let E'' be the codomain of φ and A'' the Montgomery coefficient of E''. Then we have $A''+2 = \frac{(\sqrt{A+2}+2)^2}{2\sqrt{A+2}} \in (\mathbb{F}_p^\times)^2$. Therefore, we conclude that $E' = E''$ as a Montgomery curve because E' is the unique Montgomery curve satisfying the property by which it is defined. By multiplying $A''+2$ by 4, we obtain the formula in the lemma for the case that $A+2 \in (\mathbb{F}_p^\times)^2$.

In the case that $-A+2 \in (\mathbb{F}_p^\times)^2$, we use quadratic twists. Let $E^{(t)}$ be the quadratic twist of E, i.e., the Montgomery curve with coefficient $-A$. Then there exists an isomorphism $\tau : E \to E^{(t)}; (x,y) \mapsto (-x, iy)$. Let φ be the isogeny in Proposition 4 from $E^{(t)}$ with $\alpha = \sqrt{-A+2}$, and E'' the codomain of φ. Let $E''^{(t)}$ be the quadratic twist of E'' and $\tau' : E'' \to E''^{(t)}$ be the isomorphism defined by $(x,y) \mapsto (-x, iy)$. Then the composition

$$E \xrightarrow{\tau} E^{(t)} \xrightarrow{\varphi} E'' \xrightarrow{\tau'} E''^{(t)}$$

is defined over $\mathbb{F}_p$. An easy calculation shows that the modified Montgomery coefficient of $E''^{(t)}$ is equal to (18). This proves the lemma. □

Remark 1. If $A+2 \in (\mathbb{F}_p^\times)^2$, then the isogeny in Lemma 12 sends $(1,-)$ to $(0,0)$. On the other hand, if $-A+2 \in (\mathbb{F}_p^\times)^2$, then the isogeny sends $(-1,-)$ to $(0,0)$ because we use the composition with the twist maps in this case. This means that $(1,-)$ generates $E[[2, \frac{1-\sqrt{-p}}{2}]^2]$ if $A+2 \in (\mathbb{F}_p^\times)^2$ and that $(-1,-)$ generates $E[[2, \frac{1+\sqrt{-p}}{2}]^2]$ if $-A+2 \in (\mathbb{F}_p^\times)^2$.

By using this lemma twice, we obtain a formula for the action of $\mathfrak{a}^2$. The obtained formula includes the square root of (18) in $(\mathbb{F}_p)^2$. Therefore, we need to determine whether $\sqrt{a}+4$ is a square in $\mathbb{F}_p$. The following lemma answers to it.

Lemma 13. *$\sqrt{a}+4$ is a square in $\mathbb{F}_p$ if and only if $p \equiv 15 \pmod{16}$.*

Proof. From Lemma 3 in [4], the subgroup $E(\mathbb{F}_p)[4]$ is isomorphism to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. This subgroup has order 8, so $E(\mathbb{F}_p)$ contains a point of order 8 if and only if $p \equiv 15 \pmod{16}$.

Assume $A+2 \in (\mathbb{F}_p^\times)^2$. Let $P = (1,-)$ on E. As we mentioned in Remark 1, P generates $E[[2, \frac{1-\sqrt{-p}}{2}]^2]$. Therefore, we have

$$\left(\frac{1-\sqrt{-p}}{2}\right)^2 P = O_E.$$

An easy calculation shows that

$$\frac{1-\sqrt{-p}}{2} P = \frac{p+1}{4} P.$$

Because P has order 4, this equation implies that a half of P is in $E(\mathbb{F}_p)$ if and only if $p \equiv 15 \pmod{16}$. From the arithmetic of Montgomery curves, the x-coordinate of a half of P is a root of

$$x^4 - 4x^3 - (4A+2)x^2 - 4x + 1.$$

This is decomposed as

$$(x^2 + (\sqrt{a} - 2)x + 1)(x^2 + (-\sqrt{a} - 2)x + 1). \tag{19}$$

It is easy to verify that (19) has a root in $\mathbb{F}_p$ if and only if $\sqrt{a}+4 \in (\mathbb{F}_p^\times)^2$. Assume (19) has a root x_0 in $\mathbb{F}_p$, and let Q be $(x_0, -)$ on E. Then we have $2Q = P$. Because $x_0 \in \mathbb{F}_p$, the image $\pi(Q)$ of the Frobenius is Q or $-Q$. If $\pi(Q) = -Q$, we obtain $\pi(P) = -P$ by multiplying both sides by 2. This contradicts the fact that $P \in E(\mathbb{F}_p)$. Therefore, we have $\pi(Q) = Q$, i.e., $Q \in E(\mathbb{F}_p)$. This proves the lemma for the case that $A + 2 \in (\mathbb{F}_p^\times)^2$.

For the case that $-A + 2 \in (\mathbb{F}_p^\times)^2$, we can prove the lemma by applying the same discussion to the quadratic twist of E. □

Now we obtain the following radical-isogeny formula for the action of $\mathfrak{a}^2$.

Theorem 14. *Let E' be a representative of the $\mathbb{F}_p$-isomorphism class $\mathfrak{a}^2 * E$ that is expressed as the Montgomery curve over $\mathbb{F}_p$ such that $(0,0)$ on E' generates $E'[\mathfrak{a}]$. Then the modified Montgomery coefficient of E' is*

$$\frac{(\varepsilon\sqrt[4]{a} + 2)^4}{\varepsilon\sqrt[4]{a}(\sqrt{a} + 4)}, \tag{20}$$

where $\varepsilon = -1$ if $p \equiv 7 \pmod{16}$ or $\varepsilon = 1$ if $p \equiv 15 \pmod{16}$.

Proof. From Lemma 13, we have

$$\sqrt{\frac{(\sqrt{a} + 4)^2}{\sqrt{a}}} = \frac{\varepsilon(\sqrt{a} + 4)}{\sqrt[4]{a}}.$$

By applying Lemma 12 twice, we obtain the formula in the theorem. □

As a corollary of Theorem 14, we prove a conjecture stated by [5]. In particular, we prove the following.

Corollary 15 (Conjecture 2 in [5]). *Let E be an elliptic curve defined by a Tate normal form $y^2 + xy - by = x^3 - bx^2$, $b \in \mathbb{F}_p$, and $P = (0,0) \in E$. Assume that $\mathrm{End}(E) \cong \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ and P generates $E[[2, \frac{1-\sqrt{-p}}{2}]^2]$. Then $-b$ is a square in $\mathbb{F}_p$. Moreover, the elliptic curve $E' : y^2 + xy - b'y = x^3 - b'x^2$ with*

$$b' = -\frac{\alpha(4\alpha^2 + 1)}{(2\alpha + 1)^4}, \tag{21}$$

where $\alpha = -\sqrt[4]{-b}$ if $p \equiv 7 \pmod{16}$ or $\alpha = \sqrt[4]{-b}$ if $p \equiv 15 \pmod{16}$, is a representative of the $\mathbb{F}_p$-isomorphism class $[2, \frac{1-\sqrt{-p}}{2}]^2 * E$ such that $(0,0)$ on E' generates $E'[[2, \frac{1-\sqrt{-p}}{2}]^2]$.

Proof. Note that $b \neq 0$ because E is smooth. We also note that P has order 4.

Let E_+ be the Montgomery curve with coefficient $2 + \frac{1}{4b}$ and E_- the Montgomery curve with coefficient $-(2 + \frac{1}{4b})$. There are two isomorphisms $\iota_+ : E \to E_+$ defined by

$$(x, y) \mapsto (\frac{1}{b}(x - b), \frac{1}{b\sqrt{b}}(y + \frac{x - b}{2}))$$

and $\iota_- : E \to E_-$ defined by

$$(x, y) \mapsto (-\frac{1}{b}(x - b), -\frac{1}{b\sqrt{-b}}(y + \frac{x - b}{2})).$$

(Here, we extend the symbol $\sqrt{\ }$ to $\mathbb{F}_p$. A choice of a square root is not essential since it corresponds to the composition with $[-1]$.)

Assume that $-b$ is not a square in $\mathbb{F}_p$. Then b is a square in $\mathbb{F}_p$, so the isomorphism ι_+ is defined over $\mathbb{F}_p$. Therefore we have $E_+ \in \mathcal{E}\ell\ell_p(\mathbb{Z}[\frac{1+\sqrt{-p}}{2}])$. From the assumption, the point $\iota_+(P)$ generates $E_+[[2, \frac{1-\sqrt{-p}}{2}]^2]$. However, the x-coordinate of $\iota_+(P)$ is -1. This contradicts Remark 1. Thus we conclude that $-b$ is a square in $\mathbb{F}_p$.

Because the isomorphism τ_- is defined over $\mathbb{F}_p$ and the x-coordinate of $\iota_-(P)$ is 1, the Montgomery curve E_- is in $\mathcal{E}\ell\ell_p(\mathbb{Z}[\frac{1+\sqrt{-p}}{2}])$, and the modified Montgomery coefficient of E_- is $-\frac{1}{b}$. Let E'_- be the Montgomery curve obtained by applying Theorem 14 to E_-. Then it is easy to verify that E' is $\mathbb{F}_p$-isomorphic to E'_- by an isomorphism defined as ι_-, which sends $(0, 0)$ on E' to $(1, -)$ on E'_-. This completes the proof. □

5.3 Computational Efficiency

We discuss the computational efficiency of our formulas in application to CSIDH and its variants. As in [5], we evaluate the costs of formulas by the number of exponentiations, multiplications, additions, and inversions on $\mathbb{F}_p$ and denote these by **E**, **M**, **A**, and **I**, respectively. Note that the exponent of **E** is almost the same size as p and that its cost is about $1.5 \log_2(p)\mathbf{M}$.

First, we consider the case of degree 3, i.e., compare the cost of our formula (16) with the original radical isogeny (6). The cost of our formula is $\mathbf{E} + 6\mathbf{M} + 12\mathbf{A}$, and that of the original is $\mathbf{E} + 3\mathbf{M} + 12\mathbf{A}$. Note that we count the multiplication by 2, 3, and 9 as **A**, 2**A**, and 4**A**, respectively. Our cost is 3**M** higher than the original. However, our parametrization t has the formula (9) to recover a Montgomery coefficient, which is easy to compute. On the other hand, the original radical isogeny needs transformations between a Montgomery curve and a curve used in radical isogenies of degree 3. The costs of these transformations are relatively high since these include some exponentiations. From this, our formula could be more efficient than the original in some parameters of cryptosystems. We explain this in detail below.

Let $E \in \mathcal{E}\ell\ell_p(\mathcal{O})$, ℓ be an odd prime dividing $p + 1$, and $\mathfrak{l}$ be a prime ideal above ℓ in $\mathcal{O}$. The method to compute the action of $\mathfrak{l}^n$ on E by [5] is as follows:

	Formula in [5]	Our formula
Isogeny	$\mathbf{E}+3\mathbf{M}+12\mathbf{A}$	$\mathbf{E}+6\mathbf{M}+12\mathbf{A}$
Transform from Montgomery	$>\mathbf{E}$	None
Transform to Montgomery	$>3\mathbf{E}$	$3\mathbf{M}+9\mathbf{A}+\mathbf{I}$

Table 2. The costs of 3-isogenies and transformations

1. Find a generator P of $E[\mathfrak{l}]$ on a Montgomery curve.
2. Transform the Montgomery curve to a curve with the image of P is $(0,0)$.
3. Compute an ℓ-isogeny $n-1$ times by iterating the radical-isogeny formula.
4. Compute an ℓ-isogeny with kernel $\langle(0,0)\rangle$ by Vélu's formula.
5. Transform the curve to a Montgomery form.

In the implementation [1] in [5] of CSURF, Step 2 contains $\mathbf{E}$, and Step 5 contains $3\mathbf{E}$. On the other hand, by using our formula, we do not need Step 2 and obtain the objective Montgomery coefficient by the formula (9) instead of Step 5. The cost of (9) is $3\mathbf{M}+9\mathbf{A}+\mathbf{I}$.

Table 2 shows the costs of the 3-isogenies and the transformations. (Table 2 redisplays the left half of Table 1.) Because the cost of $\mathbf{I}$ is less than that of $\mathbf{E}$, our formula reduces the cost of the transformations at least $3\mathbf{E}$. In addition, if we use the projective coordinate on Montgomery curves, then the inversion in (9) vanishes. While the exceeding cost of our formula in Step 3 is $3(n-1)\mathbf{M}$. In Step 4, both methods use Vélu's formulas. However, our method is slightly faster because Vélu's formulas on Montgomery curves are efficient. Therefore, if the exponent n of the ideal is less than about $1.5\log_2(p)$, then our formula accelerates the action of an ideal of norm 3.

Remark 2. The implementation in [5] uses 9-isogenies instead of 3-isogenies for CSURF-512, a parameter set of CSURF proposed by [4]. Since the characteristic p of the base field in CSURF-512 satisfies $9 \mid p+1$, the elliptic curves in $\mathcal{E}\ell\ell_p(\mathcal{O})$ have a point of order 9 over $\mathbb{F}_p$. In this case, using 9-isogenies reduces the cost of the action of an ideal of norm 3 since the number of $\mathbf{E}$ in Step 3 is halved. Consequently, our formula does not improve the efficiency in this case. However, our formula could do in the case that $9 \nmid p+1$, for example, CSIDH-512 proposed in [6].

Finally, we consider the cost of the formulas of 4-isogenies. The cost of our formula (20) is slightly less than that of the original formula (21) by the cost of $\mathbf{A}$. As we showed in the proof of Corollary 15, the transformations between a Montgomery curve and a Tate normal form do not need any exponentiation. Table 3 shows the formulas and the costs of the transformations. Note that we can remove $\mathbf{I}$ in line 2 and $\mathbf{M}$ in line 4 in the table if we use the projective coordinate on Montgomery curves. Whether we use the projective coordinate or not, our formula reduce the cost of the action of an ideal of norm 4.

[1] https://github.com/KULeuven-COSIC/Radical-Isogenies

	Formula	Cost
Montgomery to Tate	$A \mapsto -\frac{1}{4A+2}$	$2\mathbf{A}+\mathbf{I}$
Tate to Montgomery	$b \mapsto -2-\frac{1}{4b}$	$2\mathbf{A}+\mathbf{I}$
Montgomery to modified Montgomery	$A \mapsto 4(A+2)$	$3\mathbf{A}$
modified Montgomery to Montgomery	$a \mapsto \frac{a}{4}-2$	$\mathbf{M}+3\mathbf{A}$

Table 3. The costs of the transformations for 4-isogenies

6 Conclusion

We proposed the radical-isogeny formulas of degrees 3 and 4 on Montgomery curves. We analyzed those computational efficiencies in application to CSIDH and its variants. Because our formulas reduce the cost of transformations between elliptic curves, these could improve the efficiency of CSIDH and its variants. In particular, we showed that our formulas of degree 3 could be efficient in some cases. Our formula of degree 4 is more efficient than the original radical isogenies. In addition, we proved the conjecture on radical isogenies of degree 4, which was left open in [5].

References

1. National Institute of Standards and Technology (NIST) ”NIST Post-Quantum Cryptography Standardization”, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
2. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient isogeny based signatures through class group computations. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019. pp. 227–247. Springer International Publishing, Cham (2019)
3. Broon, F.L.P., Dang, T., Fouotsa, E., Moody, D.: Isogenies on twisted Hessian curves. Journal of Mathematical Cryptology **15**(1), 345–358 (2021), https://doi.org/10.1515/jmc-2020-0037
4. Castryck, W., Decru, T.: CSIDH on the surface. In: Ding, J., Tillich, J.P. (eds.) Post-Quantum Cryptography. pp. 111–129. Springer International Publishing, Cham (2020)
5. Castryck, W., Decru, T., Vercauteren, F.: Radical isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 493–519. Springer International Publishing, Cham (2020)
6. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018. pp. 395–427. Springer International Publishing, Cham (2018)
7. Cervantes-Vázquez, D., Chenu, M., Chi-Domínguez, J.J., De Feo, L., Rodríguez-Henríquez, F., Smith, B.: Stronger and faster side-channel protections for CSIDH. In: Schwabe, P., Thériault, N. (eds.) Progress in Cryptology – LATINCRYPT 2019. pp. 173–193. Springer International Publishing, Cham (2019)

8. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. Journal of Cryptology **22**(1), 93–113 (Jan 2009), https://doi.org/10.1007/s00145-007-9002-x
9. Costello, C., Hisil, H.: A simple and compact algorithm for SIDH with arbitrary degree isogenies. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017. pp. 303–329. Springer International Publishing, Cham (2017)
10. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291 (2006), https://eprint.iacr.org/2006/291
11. De Feo, L., Galbraith, S.D.: SeaSign: Compact isogeny signatures from class group actions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019. pp. 759–789. Springer International Publishing, Cham (2019)
12. Diamond, F., Shurman, J.: A First Course in Modular Forms. Graduate Texts in Mathematics, Springer New York (2006)
13. Feo, L.D., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology **8**(3), 209–247 (2014)
14. Fouotsa, T.B., Petit, C.: InSIDH: a simplification of sigamal. Cryptology ePrint Archive, Report 2021/218 (2021), https://eprint.iacr.org/2021/218
15. Jao, D., Azarderakhsh, R., Campagna, M., Costello, C., De Feo, L., Hess, B., Jalali, A., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Pereira, G., Renes, J., Soukharev, V., Urbanik, D.: "SIKE - Supersingular isogeny key encapsulation", Submission to the NIST Post-Quantum Cryptography Standardization project; https://sike.org
16. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.Y. (ed.) Post-Quantum Cryptography. pp. 19–34. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
17. Kim, S., Yoon, K., Park, Y.H., Hong, S.: Optimized method for computing odd-degree isogenies on Edwards curves. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019. pp. 273–292. Springer International Publishing, Cham (2019)
18. Montgomery, P.L.: Speeding the Pollard and elliptic curve methods of factorization. Mathematics of Computation **48**(177), 243–264 (1987)
19. Moriya, T., Onuki, H., Takagi, T.: SiGamal: A supersingular isogeny-based PKE and its application to a PRF. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 551–580. Springer International Publishing, Cham (2020)
20. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145 (2006), https://eprint.iacr.org/2006/145
21. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Springer New York, 2nd edn. (2009)
22. Stolbunov, A.: Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. Advances in Mathematics of Communications **4**(2), 215 (2010), http://aimsciences.org//article/id/e8001706-6615-4b24-b499-8ea9d348dabb
23. Streng, M.: Generators of the group of modular units for Gamma1(N) over QQ. arXiv:1503.08127v2 (2019), https://arxiv.org/abs/1503.08127v2
24. Vélu, J.: Isogénies entre courbes elliptiques. Comptes-Rendues de l'Académie des Sciences **273**, 238–241 (1971)