COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 68 2020

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

Symbolic Computation of Isogenies of Elliptic Curves by Vélu's Formula

by

Masayuki NORO, Masaya YASUDA, and Kazuhiro YOKOYAMA

(Received December 9, 2019)
(Revised March 17, 2020)

Abstract. We give explicit symbolic formulas of the isogeny of degree ℓ from an elliptic curve E to that $\tilde{E}$ in terms of coefficients a, b of E defined by $y^2 = x^3 + ax + b$. Since the isogeny of degree ℓ can be expressed as $\left(\frac{N_\ell}{F_\ell^2}, y(\frac{N_\ell}{F_\ell^2})'\right)$, where N_ℓ, F_ℓ are polynomials in x and N_ℓ is expressed by F_ℓ and its derivatives, we mean a symbolic formula of the isogeny by a representation of F_ℓ in terms of a, b. Considering the algebraic structure of the extended field generated by coefficients of F_ℓ and $\tilde{a}, \tilde{b}$, we show that all coefficients of F_ℓ can be expressed as certain rational functions in a, b and t_1, where t_1 is the coefficient of $x^{\frac{\ell-1}{2}-1}$ in F_ℓ. Its actual computation can be done by using a Gröbner basis of the ideal associated to such algebraic constraints derived from the well-known Vélu's formula. The correctness of our computed formulas is examined by adopting them to SEA algorithm which counts the number of rational points of an elliptic curve over a finite field.

1. Introduction

Elliptic curves have been playing an important role not only in number theory but also in related fields such as cryptography by its computational aspect. For an elliptic curve E defined over a field K, the set $E(K)$ of its K-rational points including the point at infinity forms an abelian group whose properties are very useful for computational number theory and also for cryptography. Among those properties, the order (the number of points) is the most important. For examples, in Elliptic Curve Primality Proving (ECPP) we search elliptic curves whose order is of special type and also for Elliptic Curve Cryptosystem, we need elliptic curves whose order is almost prime for making the Elliptic Curve Discrete Logarithm Problem (ECDLP) enough hard. (See textbooks [4, 27, 30].) The well-known Schoof-Elkies-Atkin (SEA) algorithm [24] and its improvements [18, 13] use explicit isogeny computation efficiently, where modular polynomials or its variants are used. Although all of computed results are exact, those are obtained by rounding approximated numerical solutions of a linear system derived from analytic properties of theory of elliptic curves. But, as an alternative, we may consider this isogeny computation in purely algebraic point of view. In more detail, by considering the extension field generated by all

coefficients appearing in the rational functions in the explicit isogeny, certain symbolic formulas can be defined with help of the action of its Galois group. For their *purely-algebraic* computation, we can use algebraic constraints on coefficients derived from the well-known Vélu's formula. We note that, once we know the shape (possible terms) of symbolic formulas, we can also apply the computational approach proposed by Charlap *et al.* [6], where finding linear relations among such possible terms can be reduced to solving a linear system derived from q-series expansions of them.

Let E and $\tilde{E}$ be elliptic curves given in explicit Weierstrass forms $y^2 = x^3 + ax + b$ and $y^2 = x^3 + \tilde{a}x + \tilde{b}$, respectively. For a positive integer ℓ, an isogeny of degree ℓ from E to $\tilde{E}$ is a rational map $\phi(x, y)$ defined over points (x, y) of E. Thanks to Vélu's theorem and its precise computational expression, for a given finite subgroup of order ℓ of E, ϕ can be expressed as

$$\phi(x, y) = \left(\frac{N_\ell(x)}{D_\ell(x)}, y \left(\frac{N_\ell(x)}{D_\ell(x)} \right)' \right),$$

where N_ℓ and D_ℓ are polynomials in x. (See [29, 5, 30].) (For a function $f(x)$ in x we denote its derivative by $f'(x)$.) As D_ℓ is a square of a polynomial F_ℓ, called the *Elkies polynomial*, of degree $(\ell - 1)/2$ in x and N_ℓ is derived from F_ℓ, F'_ℓ and F''_ℓ, computation of the isogeny is reduced to that of each coefficient of F_ℓ. Moreover the coefficients $\tilde{a}, \tilde{b}$ of $\tilde{E}$ can be also computed from coefficients of F_ℓ. Basically, the isogeny between elliptic curves $E, \tilde{E}$, can be computed efficiently in several numerical techniques. Thus, as a natural computational problem, it arises whether there is a *symbolic formula* of isogenies (coefficients of F_ℓ), where an elliptic curve is given in symbolic form, that is, in a Weierstrass form with indeterminate coefficients a, b, and if exists, how we can compute it practically. Thus, the following is set as our goal that shall contribute to computational aspect of theory of elliptic curves and its application.

1. Show that there exist explicit formulas for expressing coefficients of F_ℓ by considering the algebraic structure of the extended field generated by those coefficients.
2. Show that such explicit formulas can be computed *by solving directly a system of algebraic equations derived from the well-known Vélu's formula*. In other words, Vélu's formula is sufficient for producing symbolic formulas.
3. Moreover, exact computation of such formulas can be considered as good *test suites* for Gröbner basis (or triangular form) computation. Examine how existing efficient techniques on Gröbner basis computation can be applied effectively to isogeny computation.

We give more details. We set the Elkies polynomial as follows;

$$F_\ell(x) = x^k + t_1 x^{k-1} + \cdots + t_k,$$

where $k = \frac{\ell-1}{2}$. Then, as symbolic formulas, we consider to find *essential* algebraic relations among all coefficients $a, b, \tilde{a}, \tilde{b}, t_1, \ldots, t_k$. As seen in Schoof's paper [24], the most important coefficients are the coefficient t_1 of x^{k-1} of F_ℓ and the coefficients $\tilde{a}, \tilde{b}$ of $\tilde{E}$. Other coefficients of F_ℓ are expressed as explicit simple polynomials in these three coefficients, and their computation is very easy.

1. By purely algebraic arguments, we succeed in expressing essential algebraic relations as a *shape form* in variables $t_1, \tilde{a}, \tilde{b}, t_2, \ldots, t_k$ over $\mathbb{Q}(a, b)$. The coefficient t_1 is in *generic position* and has its minimal polynomial over $\mathbb{Q}[a, b]$ of degree $\ell + 1$. (We note that its irreducibility was already shown in [6].) Other variables $\tilde{a}, \tilde{b}, t_2, \ldots, t_k$ are expressed as polynomials in t_1 over $\mathbb{Q}(a, b)$. But, for each of their coefficients in $\mathbb{Q}(a, b)$, its denominator and numerator (in $\mathbb{Q}[a, b]$) tend to be very huge. Thus, we also present a much more concise formula called *RUR (Rational Univariate Representation)* formula. By this formula, each of variables $\tilde{a}, \tilde{b}, t_2, \ldots, t_k$ is expressed as rational functions in t_1 with small denominator (the derivative of the minimal polynomial of t_1). We note that in [6] only minimal polynomials were dealt and no algebraic relation among $t_1, \tilde{a}, \tilde{b}$ was discussed.
2. We consider the ideal generated by algebraic constraints derived from Vélu's formula. Our precise analysis on it shows that each zero of the ideal with $4\tilde{a}^3 + 27\tilde{b}^2 \neq 0$ gives exactly a correct isogeny. This implies that Vélu's formula can be considered as *a generic one* in algebraic sense.
3. Those formulas can be computed on real computer by using *efficient modular techniques* for Gröbner bases computation. Also, their computation over finite fields can be also efficiently done by using the property of *weighted* homogeneousness. Thus, in our computational experience the RUR formulas were computed successfully and verified up to $\ell = 83$.
4. In addition to the above, the computed formulas can be adopted directly to SEA algorithm of counting rational points of elliptic curves over finite fields with the same efficiency. Our implementation can compute the correct answer which guarantees the correctness of our formulas. We note that, once we succeed in getting a Gröbner basis of the ideal, we can derive any other essential relations simply by *change of order* technique. (See Section 6.)

We have to remark that our aim for construction of symbolic formulas is not to improve SEA algorithm, since polynomial factorization is inevitable for any symbolic formula. We consider simply how we can obtain essential relations by Vélu's formula and this task can be a good exercise for Gröbner basis computation. Specifically, we can apply modular techniques efficiently. Moreover, we may apply *interpolation techniques* for computing our formulas by more simplified Gröbner basis computation, where the coefficients a, b are evaluated with several integers. This might improve the total efficiency for computing our formulas. Meanwhile, as the shape of our formulas are theoretically given, we may efficiently apply the computational approach in [6], where one has to first predict the form (list up possible terms in $a, b, t_1, \tilde{a}, \tilde{b}$). As the RUR formula is concise, that is, has less number of terms, it should be suited for this computational approach. It is a very interesting task to make this application very efficient and some possible combination among this approach and Gröbner basis computation can be considered. These improvements should be our next work for computing our formulas for larger ℓ.

At the end, we would like to give one more remark on possible contribution to theory of elliptic curves. In order to express formulas in a *shape form* or an *RUR*, we review theoretical results on elliptic curves over $\mathbb{C}$ and translate them to their counterparts on

elliptic curves over $\mathbb{C}(a, b)$, the rational function field in two variables over $\mathbb{C}$. By this translation, we merely consider certain *generic case*, where the Galois group acts on $E[\ell]$ as the general linear group $GL(2, \ell)$, where $E[\ell]$ denotes the ℓ-torsion subgroup of E, that is, the unique subgroup of E with order ℓ^2. Usually, many studies were done on elliptic surfaces which are defined over the rational function field in one variable, and our setting in several variables is quite special. But, we hope that our simple study could be the first step for making fruitful results in elliptic curves over rational function fields in several variables. We also remark that, from the computed formulas, we found some interesting numerical properties on our formulas, which will be given in Appendix.

The rest of this paper is organized as follows. Section 2 provides necessary mathematical fundamentals on computational aspects on isogeny. We give a further study on algebraic properties of coefficients of F_ℓ. Section 3 extends properties discussed in Section 2 to their counterparts in parametric case, that is, elliptic curves with indeterminate coefficients. Then our symbolic formulas are defined explicitly in purely algebraic manner. Section 4 explains how symbolic and algebraic methods can be applied for computing our symbolic formulas. We characterize the algebraic structure of the ideal associated to the system of algebraic equations derived from Vélu's formula. Section 5 gives how efficient techniques on Gröbner bases computation can be applied and how large degree we can succeed in getting formulas. We show the state-of-arts on computation of symbolic formulas. Also Section 6 reports that our formulas can be effectively adopted to SEA algorithm. Section 7 summarizes our results and computational observation for further development. Also, in Appendix, we give computed examples and some numerical properties found from our computed example. We remark that all formulas were computed by using *Risa/Asir* computer algebra system, and their binary data can be downloaded from the page: http://www2.rikkyo.ac.jp/web/noro/isogeny.

2. Preliminaries on Computational Aspect on Isogeny

In this section, we review basic properties of isogenies of an odd prime degree ℓ. Here we use the standard notations on elliptic curves. (See textbooks [27, 30].) Let K be a field and $\overline{K}$ denote its algebraic closure. Let E and $\widetilde{E}$ be two elliptic curves defined over $\overline{K}$. An *isogeny* between E and $\widetilde{E}$ is a regular rational map $\phi : E \longrightarrow \widetilde{E}$ that induces a group homomorphism $E \longrightarrow \widetilde{E}$. Throughout this paper, we assume that all isogenies are non-zero and separable. Then $\widetilde{E} \simeq E/S$, where S is the finite kernel of ϕ. Since ϕ is separable, the *degree* of ϕ is defined as $\deg \phi = [\overline{K}(E) : \phi^*\overline{K}(\widetilde{E})] = \#S$, where $\phi^* : \overline{K}(\widetilde{E}) \longrightarrow \overline{K}(E)$ is the induced map between function fields $\overline{K}(E)$ and $\overline{K}(\widetilde{E})$.

2.1. Isogeny and Vélu's Formula

From now on, we express an elliptic curve by its Weierstrass equation. Let E be an elliptic curve defined by $y^2 = x^3 + ax + b$ over K, that is, $a, b \in K$, and ℓ an odd prime. For cases we need to distinguish elliptic curves, we write $E(a, b)$. Also, for each $P \in E \setminus \{\infty\}$, where ∞ denotes the point at infinity, we denote its x coordinate by $x(P)$ and its y coordinate by $y(P)$. We assume $\mathrm{char}(K)$ is 0 or sufficiently larger than ℓ. Therefore, any isogeny of degree ℓ is separable. Let S denote a subgroup of E of order ℓ. Then S is a subgroup of

the ℓ-torsion subgroup $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$ and there are $\ell + 1$ such subgroups of order ℓ.

Vélu [29] showed how to explicitly represent the rational function of the isogeny $\phi : E \longrightarrow \widetilde{E} = E/S$. Based on independent works by [16] and [9], Bostan *et al.* [5] showed that a normalized isogeny ϕ can be written as follows: An isogeny $\phi : E \longrightarrow \widetilde{E}$ is said to be *normalized* if $\phi^*(\omega_{\widetilde{E}}) = \omega_E$, where ω_E and $\omega_{\widetilde{E}}$ denote the invariant differentials of E and $\widetilde{E}$, respectively.

PROPOSITION 2.1 (Modified Vélu's formula [5]:Proposition 4.1). *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over a field K, ℓ an odd prime, and $\phi : E \longrightarrow \widetilde{E}$ a normalized isogeny of degree ℓ and S its kernel. Then ϕ can be written as*

$$\phi(x, y) = \left(\frac{N_\ell(x)}{D_\ell(x)}, y \left(\frac{N_\ell(x)}{D_\ell(x)} \right)' \right), \tag{1}$$

where the polynomial $D_\ell(x)$ is given by

$$D_\ell(x) = \prod_{P \in S \setminus \{\infty\}} (x - x(P)) = x^{\ell-1} - s_1 x^{\ell-2} + s_2 x^{\ell-3} - \cdots + s_{\ell-1} \tag{2}$$

and $N_\ell(x)$ is related to $D_\ell(x)$ through the formula

$$\frac{N_\ell(x)}{D_\ell(x)} = \ell x - s_1 - (3x^2 + a)\frac{D'_\ell(x)}{D_\ell(x)} - 2(x^3 + ax + b)\left(\frac{D'_\ell(x)}{D_\ell(x)} \right)'. \tag{3}$$

Addition to Proposition 2.1, we give more details. Let

$$F_\ell(x) = \prod_{P \in S^+} (x - x(P)) = x^k + t_1 x^{k-1} + \cdots + t_k, \tag{4}$$

where $S \setminus \{\infty\}$ is partitioned into S^+ and S^- such that $S = \{\infty\} \cup S^+ \cup S^-$ and $S^- = \{-P : P \in S^+\}$. Then $k = \frac{\ell-1}{2}$, $D_\ell(x) = F_\ell(x)^2$ and $s_1 = -2t_1$ since ℓ is an odd prime. According to [18], we call F_ℓ the *ℓ-th Elkies polynomial*. Then $N_\ell(x)$ can be expressed by using $F_\ell(x)$ as

$$N_\ell(x) = (\ell x + 2t_1)F_\ell(x)^2 - 2(3x^2 + a)F'_\ell(x)F_\ell(x) - 4(x^3 + ax + b)(F''_\ell(x)F_\ell(x) - F'_\ell(x)^2). \tag{5}$$

Moreover, we have the following relations:

$$\begin{cases} \tilde{a} = (1 - 10k)a - 30t_1^2 + 60t_2, \\ \tilde{b} = (1 - 28k)b + 70t_1^3 - 210t_1t_2 + 210t_3 + 42at_1. \end{cases} \tag{6}$$

As $N_\ell(x)$, $D_\ell(x)$, $F_\ell(x)$ are determined by the choice of the subgroup S, we also write them by $N_\ell^S(x)$, $D_\ell^S(x)$, $F_\ell^S(x)$. Also, for $F_\ell^S(x)$, we write t_i^S for its coefficient of x^i. Thus,

$$F_\ell^S(x) = x^k + t_1^S x^{k-1} + \cdots + t_k^S.$$

By (6), the coefficients $\tilde{a}, \tilde{b}$ are determined by a, b, t_1, t_2 and t_3, and thus they are determined by S. Therefore, we also write $\tilde{a}^S$ and $\tilde{b}^S$.

REMARK 2.2. For our symbolic computation, we consider $a, b, t_1, \ldots, t_k$ as variables and introduce weights on $x, a, b, t_1, \ldots, t_k$ such that the weight of x is 1, that of s_1 is 1, that of a is 2, that of b is 3, and for each i, $1 \leq i \leq k$, that of t_i is i. Then, $F_\ell(x)$, $D_\ell(x)$ and $N_\ell(x)$ are weighted homogeneous polynomials. Their weights are k, $2k$ and $\ell(= 2k + 1)$, respectively.

REMARK 2.3. We can examine whether ϕ maps the point at infinity of E to that of $\tilde{E}$ by simply checking the degrees and leading coefficients of polynomials appearing in Equation (1). Considering the projective coordinate, we may write a point by $[x, y, z]$, where $[0, 1, 0]$ implies the point at infinity. (We use the notation in Chapter I in [27].) Then the map $\phi(x, y)$ can be rewritten in a projective form as

$$\phi([x, y, z]) = \left[F_\ell^*(x, z)N_\ell^*(x, z),\ y(N_\ell' F_\ell - 2N_\ell F_\ell')^*(x, z),\ z(F_\ell^*(x, z))^3\right],$$

where G^* denotes the homogenization of a polynomial G with respect to z. However, it cannot map the point at infinity $[0, 1, 0]$, and so it can not be proven even to be a morphism by its shape. Thus, we modify the map slightly as follows.

It is clear that $F_\ell(x)$ is monic and of degree k and its square $D_\ell(x)$ is also monic and of degree $2k$. Also, by seeing the leading coefficients of the right hand side of Equation (5), it follows that $N_\ell(x)$ is monic and of degree $\ell = 2k + 1$ and $N_\ell' F_\ell - 2N_\ell F_\ell'$ is also monic and of degree $3k$. Dividing $N_\ell' F_\ell - 2N_\ell F_\ell'$ by $x^3 + ax + b(= y^2)$, we can express it as a polynomial $M(x, y)$ in x, y as follows;

$$M(x, y) = y^{2k} + M_1(x)y^{2k-2} + \cdots + M_{k-1}(x)y^2 + M_k(x),$$

where each M_i is a polynomial in x of degree less than 3. In the same manner, we rewrite other polynomials $F_\ell N_\ell$ and F_ℓ^3 as $U(x, y)$ and $V(x, y)$, respectively. Then we have

$$\begin{aligned} U(x, y) &= (x + U_0)y^{2k} + U_1(x)y^{2k-2} + \cdots + U_{k-1}(x)y^2 + U_k(x), \\ V(x, y) &= y^{2k} + V_1(x)y^{2k-2} + \cdots + V_{k-1}(x)y^2 + V_k(x), \end{aligned}$$

where U_0 is a constant and U_i, V_i are polynomials in x of degree less than 3. We note that the total degree of $M(x, y)$ is $2k$, that of $U(x, y)$ is $2k + 1$ and that of $V(x, y)$ is $2k$. Moreover, it is clear that they give the same values as their corresponding polynomials on E. Thus, to handle the point at infinity $[0, 1, 0]$, we consider the following *equivalent* map ϕ_0

$$\phi_0([x, y, z]) = \left[U^*(x, y, z),\ yM^*(x, y, z),\ zV^*(x, y, z)\right].$$

As $U^*(0, 1, 0) = 0$ and $M^*(0, 1, 0) = 1$, it maps the point at infinity of E to that of $\tilde{E}$.

2.2. Algebraic Structures Related to Vélu's Formula

We extract some useful properties on algebraic structures related to $E[\ell]$ and $t_1, \ldots, t_k$, $\tilde{a}, \tilde{b}$. We begin by recalling properties of division polynomials. The map ϕ_n which multiplies all points of E by n is an important isogeny. It can be written explicitly as a rational map by using division polynomials ψ_i given in Definition 2.4 as follows (see Section 3.2 in [30] for details):

$$\phi_n : E(K) \ni P = (x, y) \mapsto nP = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2},\ \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3}\right). \quad (7)$$

DEFINITION 2.4. The ℓ th division polynomial ψ_ℓ is defined in a recursive manner as follows:

$$\begin{cases} \psi_0 = 0\,, \\ \psi_1 = 1\,, \\ \psi_2 = 2y\,, \\ \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2\,, \\ \psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)\,, \\ \psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2 \\ \psi_{2m} = (2y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m \text{ for } m \geq 3 \end{cases}$$

We note that ψ_{2m+1} is a polynomial in x over K by replacing y^2 with $x^3 + ax + b$. Then, it is shown that for an odd prime ℓ, ψ_ℓ is the polynomial in x whose roots are x-coordinates of ℓ-torsion points in $E[\ell] \setminus \{\infty\}$. Thus, all roots of $\psi_\ell(x)$ are algebraic over K. Moreover, since roots of ψ_ℓ are x-coordinates of points in $E[\ell]$, as long as $E(a, b)$ is an elliptic curve, that is, $4a^3 + 27b^2 \neq 0$, ψ_ℓ is square-free by looking its degree shown in the following lemma which can be shown easily by induction argument. *This implies that the discriminant of $\psi_\ell(x)$ is a power of $4a^3 + 27b^2$ with some non-zero leading coefficient.*

LEMMA 2.5. *The degree of $\psi_\ell(x)$ is $\frac{\ell^2-1}{2}$ and its leading coefficient is ℓ. Moreover the coefficient of $x^{\frac{\ell^2-3}{2}}$ (the second term) in $\psi_\ell(x)$ is* 0.

As $E[\ell]$ has $\ell + 1$ subgroups of order ℓ, let $S_1 (= S), \ldots, S_{\ell+1}$ be all those subgroups. Then, for each S_i, we have the polynomial $F_\ell^{S_i}$ by Proposition 2.1 and

$$\psi_\ell(x) = \ell \prod_{i=1}^{\ell+1} F_\ell^{S_i}(x)\,.$$

As shown in (6), each t_i can be written by a symmetric polynomial of degree i in all roots of $F_\ell(x)$, t_i is also algebraic over K. Moreover, $\tilde{a}$ is written as a polynomial in t_1, t_2 over K and $\tilde{b}$ is written as a polynomial in t_1, t_2, t_3 over K. (See (6).) Thus they are also algebraic over K.

LEMMA 2.6. *All t_i are algebraic over K and also the coefficients $\tilde{a}, \tilde{b}$ of $\tilde{E}$ are algebraic over K. (The same holds for $t_i^{S_j}$, $\tilde{a}^{S_j}$ and $\tilde{b}^{S_j}$.)*

For computation of $F_\ell(x), \tilde{a}, \tilde{b}$, we need certain field extension. In fact, the extension field $L = K(t_1, t_2, \ldots, t_k, \tilde{a}, \tilde{b})$ is the smallest extension field for the computation. We also write L^{S_i} for $K(t_1^{S_i}, t_2^{S_i}, \ldots, t_k^{S_i}, \tilde{a}^{S_i}, \tilde{b}^{S_i})$.

Let $K(E[\ell])$ be the extension field of K generated by $\{x(P), y(P) \mid P \in E[\ell] \setminus \{\infty\}\}$. As the group addition can be written as a rational function over K, each element of the Galois group $Gal(K(E[\ell])/K)$ acts on $E[\ell]$ as a *linear map*, where $E[\ell]$ is considered as a 2-dimensional vector space over $\mathbb{F}_\ell$. Thus, $Gal(K(E[\ell])/K)$ can be considered as a subgroup of $GL(2, \ell)$. For $K = \mathbb{Q}$, there is a *Serre* curve $E = E(a_0, b_0)$ such that the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell]$ is exactly isomorphic to $GL(2, \ell)$. (For Serre curves,

see [25, 15] and [7], where elliptic curves over a univariate function field are considered.) For simplicity, we denote $Gal(K[E[\ell]/K)$ by G_ℓ.

Now we consider the case where $G_\ell \cong GL(2, \ell)$. Recall that $S = S_1, \ldots, S_{\ell+1}$ are all distinct subgroups of order ℓ of $E[\ell]$. Then, G_ℓ acts on transitively on $E[\ell] \setminus \{\infty\}$ and so on $x(E[\ell]) = \{x(P) \mid P \in E[\ell] \setminus \{\infty\}\}$. We note that $\#x(E[\ell]) = \frac{\ell^2-1}{2}$ as two points have the same x coordinates. Also, the kernel of its action on $x(E[\ell])$ is $\{\pm 1\}$. It can be shown as follows. Choosing a basis $\{P, P'\}$ of $E[\ell]$ as a vector space, each element σ of the kernel transforms P to $\pm P$ and P' to $\pm P'$. If σ transforms P to P and P' to $-P'$, then it transforms $P + P'$ to $P - P'$. As σ fixes $x(P)$, $x(P')$ and $x(P + P')$, this implies $x(P + P') = x(P - P')$ and so $P + P' = P - P'$ or $P + P' = -P + P'$. Thus $2P = \infty$ or $2P' = \infty$. As $\ell > 2$, this is a contradiction.

Since each subgroup S_i of order ℓ is considered as a *line*, $x(S_i) = \{x(P) \mid P \in S_i \setminus \{\infty\}\}$ forms an *imprimitive block*. Since $G_\ell \cong GL(2, \ell)$ acts transitively on the set of all lines, G_ℓ acts transitively on those imprimitive blocks. For the set-wise stabilizer $Stab_{G_\ell}(S_i)$ of S_i in G_ℓ, $Stab_{G_\ell}(S_i)$ acts on S_i transitively and so on $x(S_i)$ transitively. Then, $Stab_{G_\ell}(S_i)$ stabilizes all symmetric polynomials in $x(S_i)$, which implies that it also stabilizes all $t_j^{S_i}$ and $\tilde{a}^{S_i}, \tilde{b}^{S_i}$. Thus, we have the following.

LEMMA 2.7. *Suppose that $G_\ell \cong GL(2, \ell)$. Then, the following results hold:*

(1) *$\psi_\ell(x)$ is irreducible over K.*
(2) *G_ℓ acts on $x(E[\ell]) = \{x(P) \mid P \in E[\ell] \setminus \{\infty\}\}$ as $GL(2, \ell)/Z_2$, where $Z_2 = \{\pm 1\}$. (We note $\#x(E[\ell]) = \frac{\ell^2-1}{2}$ and $x(E[\ell])$ coincides with the set of all roots of $\psi_\ell(x)$.)*
(3) *The set $\{x(S_1), x(S_2), \ldots, x(S_{\ell+1})\}$ forms a system of imprimitive blocks of the action of G_ℓ.*
(4) *$F_\ell^{S_1}, \ldots, F_\ell^{S_{\ell+1}}$ are conjugate to each other, where G_ℓ acts naturally on the polynomial ring $K(E[\ell])(x)$.*
(5) *The stabilizer $Stab_{G_\ell}(L)$ of L in G_ℓ coincides with the set-wise stabilizer $Stab_{G_\ell}(S)$, where G_ℓ acts on $E[\ell]$ as the linear map $GL(2, \ell)$ and S is a line in $E[\ell]$. This implies that the extension degree of L/K is $\ell + 1$. (The same holds for L^{S_i}.)*

For many examples, t_1 is a primitive element of L, that is, $L = K(t_1)$. In these cases, all other elements $t_2, \ldots, t_k$ and $\tilde{a}, \tilde{b}$ are expressed as polynomials in t_1 over K. Actually, in our case, if $t_1 \neq 0$, t_1 is a primitive element.

LEMMA 2.8. *Suppose that $G_\ell \cong GL(2, \ell)$. If $t_1 (= t_1^{S_1}) \neq 0$, then $t_1^{S_1} (= t_1), \ldots, t_1^{S_{\ell+1}}$ are all distinct. This means that the extension degree of $K(t_1)/K$ is $\ell + 1$ and $L = K(t_1)$.*

Proof. Suppose that $t_1 \neq 0$. As $s_1 = s_1^S$, where $S = S_1$, is the sum of all x coordinates of points in $S \setminus \{\infty\}$ and $-t_1$ is a half of s_1, $t_1 = -\sum_{u \in x(S)} u$. By Lemma 2.7 each $x(S_i)$ forms an imprimitive block. This means that, for P in $S_i \setminus \{\infty\}$, the stabilizer $Stab_{G_\ell}(x(P))$ of $x(P)$ in G_ℓ also stabilizes the set $x(S_i)$ and so $t_1^{S_i}$. Thus, the stabilizer $Stab_{G_\ell}(t_1^{S_i})$ of $t_1^{S_i}$ in G_ℓ contains $Stab_{G_\ell}(x(P))$.

Now we show that $t_1^{S_i} \neq t_1^{S_j}$ for $1 \leq i \neq j \leq \ell+1$. Suppose, to the contrary, that there are different subgroups, say T, T', such that $t_1^T = t_1^{T'}$. Then, we take a point P in $T \setminus \{\infty\}$. By the action of $GL(2,\ell)$, $Stab_{G_\ell}(x(P))$ also acts transitively on $\{x(P') \mid P' \in E[\ell] \setminus T\}$. This implies that $Stab_{G_\ell}(t_1^T)$ acts transitively on $\{x(P') \mid P' \in E[\ell] \setminus T\}$ and also transitively on $\{x(T'') \mid T'' \neq T\}$. Thus, it transforms $t_1^{T'}$ to $t_1^{T''}$ for any subgroup $T'' \neq T$ of order ℓ. But, as it stabilizes $t_1^{T'} (= t_1^T)$, we conclude that $t_1^T = t_1^{T''}$ for any subgroup T'' of order ℓ. As the coefficient of the second leading term $x^{\frac{\ell^2-3}{2}}$ in $\psi_\ell(x)$ is the sum of all $t_1^{S_i}$, it should coincides with $(\ell+1)t_1$. But, by Lemma 2.5 it is 0 and so t_1 should be 0. This is a contradiction. □

3. Symbolic Formulas of Isogeny

Here we give the definition of *symbolic formulas* of isogeny.

3.1. Algebraic Structures in Parametric Case

For *symbolic computation of isogeny*, we consider a, b as variables (parameters). Here we use the same notation as in the previous section. Then, $\psi_\ell(x)$ is a polynomial in x, a, b over K and we consider x as its main variable. To indicate variables a, b explicitly, we write $\psi_\ell(x; a, b)$. (We use the same for other polynomials.) By the weight defined in Remark 2.2, we have the following:

LEMMA 3.1. *$\psi_\ell(x; a, b)$ is weighted homogeneous of weight $\frac{\ell^2-1}{2}$. Moreover, as $4a^3 + 27b^2 \neq 0$ in $K(a, b)$, $\psi_\ell(x; a, b)$ is square-free.*

By Lemma 2.6, all t_i's and $\tilde{a}, \tilde{b}$ are shown to be algebraic over K. When a, b are variables, we can show more precise properties over $K(a, b)$. We recall that $K[a, b]$ is an integrally closed domain in $K(a, b)$, as it is a UFD. (See (13.3) in [20].) As $\psi_\ell(x; a, b)$ is a polynomial in x over $K[a, b]$ with leading coefficient ℓ, all roots of $\psi_\ell(x; a, b)$ are *integral* over $K[a, b]$. Then, since each t_i is expressed as an integral polynomial in elementary symmetric forms in roots of $\psi_\ell(x; a, b)$, it is also integral over $K[a, b]$. Moreover, since $\tilde{a}$ and $\tilde{b}$ are expressed as polynomials in t_1, t_2, t_3 over $K[a, b]$ (see the formula (6)), they are also integral over $K[a, b]$. By this fact, their minimal (monic) polynomials over $K(a, b)$ have *integral* coefficients, that is, those are defined over $K[a, b]$.

LEMMA 3.2. *$t_1, \tilde{a}$ and $\tilde{b}$ are all integral over $K[a, b]$ and their minimal polynomials $m_{t_1}(x)$, $m_{\tilde{a}}(x)$ and $m_{\tilde{b}}(x)$ over $K(a, b)$ are defined over $K[a, b]$.*

Now we consider the case $K = \mathbb{Q}$ and the smallest field $L = \mathbb{Q}(a, b)(t_1, \ldots, t_k, \tilde{a}, \tilde{b})$ over which F_ℓ and $\tilde{a}, \tilde{b}$ are defined. The following lemmas give alternative proofs for theorems in Appendix of [6] about the irreducibility of ψ_ℓ and the degree of m_{t_1}.

LEMMA 3.3. *$\psi_\ell(x; a, b)$ is irreducible over $\mathbb{Q}(a, b)$ and its Galois group over $\mathbb{Q}(a, b)$ is isomorphic to $GL(2, \ell)/Z_2$. Moreover, the extension degree $L/\mathbb{Q}(a, b)$ is $\ell+1$.*

Proof. First we show that $\psi_\ell(x; a, b)$ is irreducible over $\mathbb{Q}(a, b)$. By Gauss' lemma, since $\psi_\ell(x; a, b)$ is a polynomial in x over $K[a, b]$, if it has a non-trivial factorization over

$K(a, b)$, that is,

$$\psi_\ell(x; a, b) = h_1(x; a, b) \times h_2(x; a, b)\,,$$

then $h_1(x; a, b)$ and $h_2(x; a, b)$ can be considered as polynomials in x over $K[a, b]$. As the leading coefficient of $\psi_\ell(x; a, b)$ belongs to K, the leading coefficient of $h_i(x; a, b)$ also belongs to K. Then, for any values a_0, b_0 in K, we have a non-trivial factorization as

$$\psi_\ell(x; a_0, b_0) = h_1(x; a_0, b_0) \times h_2(x; a_0, b_0)\,.$$

We note that degrees of ψ_ℓ, h_1, h_2 are unchanged by the substitution.

Thus, if there are some special values a_0, b_0 in K such that $\psi_\ell(x; a_0, b_0)$ is irreducible, we have a contradiction to prove the irreducibility of $\psi_\ell(x; a, b)$. As mention in previous subsection, there exists a *Serre* curve $E = E(a_0, b_0)$ such that the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell]$ is isomorphic to $GL(2, \ell)$, where $E[\ell]$ is considered as a 2-dimensional vector space over $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$. In this case, by Lemma 2.7 $\psi_\ell(x; a_0, b_0)$ is irreducible over $\mathbb{Q}$.

In the same manner, we can show that the Galois group of $\psi_\ell(x; a, b)$ over $\mathbb{Q}(a, b)$ is isomorphic to $GL(2, \ell)/Z_2$ by considering *resolvents* over $\mathbb{Q}(a, b)$. We recall that from the action of $GL(2, \ell)$ on $E[\ell]$, $GL(2, \ell)$ acts on $x(E[\ell]) = \{x(P) \mid P \in E[\ell] \setminus \{\infty\}\}$, where its kernel is $\{\pm 1\}$, and the action of $GL(2, \ell)$ on $x(E[\ell])$ is considered as $GL(2, \ell)/Z_2$. (See Lemma 2.7 (2).)

Now we use the following property: (See Section 3.3 in [14].) Suppose that $f(x; \boldsymbol{t})$ is monic and irreducible over $\mathbb{Q}(\boldsymbol{t})[x]$, where $\boldsymbol{t}$ is a set of parameters (variables). Then, for any values $\boldsymbol{t}_0$ over $\mathbb{Q}$, if $f(x; \boldsymbol{t}_0)$ is square-free,

$$Gal(f(x; \boldsymbol{t}_0)/\mathbb{Q}) \subset Gal(f(x; \boldsymbol{t})/\mathbb{Q}(\boldsymbol{t}))\,,$$

where $Gal(f(x; \boldsymbol{t}_0)/\mathbb{Q})$ denotes the Galois group of $f(x; \boldsymbol{t}_0)$ over $\mathbb{Q}$ and $Gal(f(x; \boldsymbol{t})/\mathbb{Q}(\boldsymbol{t}))$ denotes the Galois group of $f(x; \boldsymbol{t})$ over $\mathbb{Q}(\boldsymbol{t})$.

For our case, there are special values a_0, b_0 giving a Serre curve $E = E(a_0, b_0)$ such that $Gal(\mathbb{Q}(E(a_0, b_0)[\ell])/\mathbb{Q}) \cong GL(2, \ell)$ and so $Gal(\psi_\ell(x; a_0, b_0)/\mathbb{Q}) \cong GL(2, \ell)/Z_2$. Thus, we have

$$GL(2, \ell)/Z_2 \cong Gal(\psi_\ell(x; a_0, b_0)/\mathbb{Q}) \subset Gal(\psi_\ell(x; a, b)/\mathbb{Q}(a, b))\,.$$

On the other hand, any field automorphism preserves point addition of $E[\ell]$ and thus

$$Gal(\psi_\ell(x; a, b)/\mathbb{Q}(a, b)) \subset GL(2, \ell)/Z_2\,.$$

Therefore, we have $Gal(\psi_\ell(x; a, b)/\mathbb{Q}(a, b)) \cong GL(2, \ell)/Z_2$. By using the same argument in the proof of Lemma 2.7, from the action of $Gal(\psi_\ell(x; a, b)/\mathbb{Q}(a, b))$ on $x(S)$, it follows that the extension degree $L/\mathbb{Q}(a, b)$ is $\ell + 1$. □

Next we consider t_1, the coefficient of x^{k-1} of $F_\ell(x)$. As $Gal(\psi_\ell(x; a, b)/\mathbb{Q}(a, b))$ is isomorphic to $GL(2, \ell)/Z_2$, by using the same argument in Lemma 2.8, we have the following.

LEMMA 3.4. *If* $t_1 \neq 0$, $t_1^{S_1}(= t_1), \ldots, t_1^{S_{\ell+1}}$ *are all distinct. This means* $\mathbb{Q}(a, b)(t_1, \ldots, t_k, \tilde{a}, \tilde{b}) = \mathbb{Q}(a, b)(t_1)$ *and the minimal polynomial of* t_1 *over* $\mathbb{Q}(a, b)$ *is of degree* $\ell + 1$.

In our case $K = \mathbb{Q}(a, b)$, we can show $t_1 \neq 0$ with help of analytic arguments in [24].

LEMMA 3.5. *In $\mathbb{Q}(a,b)$, $t_1 \neq 0$. Thus, $\mathbb{Q}(a,b)(t_1,\ldots,t_k,\tilde{a},\tilde{b}) = \mathbb{Q}(a,b)(t_1)$ and the minimal polynomial of t_1 over $\mathbb{Q}(a,b)$ is of degree $\ell+1$.*

Proof. Suppose, to the contrary, that $t_1 = 0$ over $\mathbb{Q}(a,b)$. We recall the formula (7). Then, t_1 can be expressed as a rational function in $x(P) \in x(S)$ over $\mathbb{Q}[a,b]$ as follows, where we write x for $x(P)$;

$$t_1(x) = x(P) + x(2P) + \cdots + x(kP) = x + \sum_{i=2}^{k}\left(x - \frac{\psi_{i-1}(x)\psi_{i+1}(x)}{\psi_i^2(x)}\right)$$
$$= \frac{kx\theta(x) + \sum_{i=2}^{k}(\frac{\theta}{\psi_i^2}(x)\psi_{i-1}(x)\psi_{i+1}(x))}{\theta(x)},$$

where $\theta(x) = \prod_{i=2}^{k}\psi_i(x)^2$. Let $\mathcal{N}_\ell(x;a,b)$ be the numerator of the rational function. Then $\mathcal{N}_\ell(x;a,b)$ is a polynomial in x over $\mathbb{Q}[a,b]$. Since each ψ_i is irreducible over $\mathbb{Q}(a,b)$, if $t_1 = 0$ over $\mathbb{Q}(a,b)$ then $t_1^{S_i} = 0$ for every S_i and $\mathcal{N}_\ell(x;a,b)$ should be divided by $\psi_\ell(x;a,b)$. As both $\mathcal{N}_\ell(x;a,b)$ and $\psi_\ell(x;a,b)$ are polynomials in x over $\mathbb{Q}[a,b]$, its cofactor $\mathcal{M}_\ell(x;a,b)$ is also a polynomial in x over $\mathbb{Q}[a,b]$. Thus, we have the following equation over $\mathbb{Q}[a,b]$ which holds for every values a,b in $\mathbb{C}$;

$$\mathcal{N}_\ell(x;a,b) = \mathcal{M}_\ell(x;a,b) \times \psi_\ell(x;a,b).$$

Hence, if there are values a_0, b_0 in $\mathbb{C}$ with $4a_0^3 + 27b_0^2 \neq 0$ such that $t_1 \neq 0$ for $E(a_0,b_0)$, then we have a contradiction. This is because for any root γ of $\psi_\ell(x;a_0,b_0)$, $\mathcal{N}_\ell(\gamma;a_0,b_0)$ should be 0 and so $t_1 = 0$.

Schoof [24] gave an analytic presentation on isogeny of degree ℓ, and he considered an elliptic curve $E\left(-\frac{E_4(q)}{48}, \frac{E_6(q)}{864}\right)$, where E_4, E_6 are Eisenstein power series of weight 4 and 6, respectively, $q = e^{2\pi\sqrt{-1}\tau}$ and $\tau \in \mathbb{C}$. (See [26, 4] for Eisenstein power series.) In this case, t_1 can be expressed by using another Eisenstein power series $E_2(q)$ as follows:

$$t_1 = -\frac{s_1}{2} = -\frac{1}{24}\ell(E_2(q) - \ell E_2(q^\ell)).$$

Comparing q-expansions of $E_2(q)$ and $E_2(q^\ell)$, it can be shown that t_1 is not a identically zero-function, which implies that there is a value q_0 such that $t_1 \neq 0$. □

3.2. Definition of Symbolic Formulas

We consider the representation $L(= \mathbb{Q}(a,b)(t_1)) \cong \frac{\mathbb{Q}(a,b)[t_1]}{\langle m_{t_1}(t_1)\rangle}$, where $\langle m_{t_1}\rangle$ denotes the ideal generated by m_{t_1}. Using a *usual elementary argument based on discriminant in field theory*, since $\mathbb{Q}[a,b]$ is integrally closed in its quotient field $\mathbb{Q}(a,b)$, it can be shown easily that the integral closure of $\mathbb{Q}[a,b]$ in L is contained in $\frac{1}{\mathrm{disc}(m_{t_1})}\mathbb{Q}[a,b][t_1]$, where $\mathrm{disc}(m_{t_1})$ denotes the discriminant of $m_{t_1}(t_1)$. (See Theorem 10.15 in [20].) More precisely, as $\mathbb{Q}[a,b]$ is a UFD, the integral closure is included in $\frac{1}{d_{t_1}}\mathbb{Q}[a,b][t_1]$, where d_{t_1} denotes the product of all square-factors of $\mathrm{disc}(m_{t_1})$. We note that $\mathrm{disc}(m_{t_1})$ and d_{t_1} are polynomials in a,b over $\mathbb{Q}$, as $m_{t_1}(t_1)$ is a polynomial in a,b,t_1 over $\mathbb{Q}$ and monic with respect to t_1. As to other $t_2,\ldots,t_k,\tilde{a},\tilde{b}$, since they are all integral over $\mathbb{Q}[a,b]$, they can be expressed as polynomials in t_1 over $\frac{1}{d_{t_1}}\mathbb{Q}[a,b]$. Hence, we have the following:

THEOREM 3.6 (Shape Form Formula). *There are polynomials $T_2, \ldots, T_k$, A, B in t_1, a, b and polynomials $d_{T_2}, \ldots, d_{T_k}$, d_A, d_B in a, b which are factors of d_{t_1} over $\mathbb{Q}$ such that*

$$\begin{cases} t_2 = \dfrac{T_2(t_1; a, b)}{d_{T_2}(a, b)}, t_3 = \dfrac{T_3(t_1; a, b)}{d_{T_3}(a, b)}, \ldots, t_k = \dfrac{T_k(t_1; a, b)}{d_{T_k}(a, b)}, \\ \tilde{a} = \dfrac{A(t_1; a, b)}{d_A(a, b)}, \tilde{b} = \dfrac{B(t_1; a, b)}{d_B(a, b)}. \end{cases} \tag{8}$$

We can assume that all rational functions are reduced and degrees of $T_2, \ldots, T_k$, A, B in t_1 are less than $\ell + 1$.

The formulas (8) with the minimal polynomial $m_{t_1}(t_1)$ can be considered as *Symbolic Formula for the isogeny of degree ℓ*. As the shape of the formula just corresponds to so-called a *shape form* in theory of Gröbner basis, we may call this formula *Shape Form formula*.

REMARK 3.7. The discriminant $\mathrm{disc}(m_{t_1})$ is calculated (up to sign) as the resultant of m_{t_1} and its derivative m'_{t_1}, that is, the determinant of the Sylvester matrix of them. Then it follows that $\mathrm{disc}(m_{t_1})$ is weighted homogeneous and its weight is $\ell(\ell+1)$. Since a factor of a weighted homogeneous polynomial is weighted homogeneous, $d_A, d_B, d_{T_2}, \ldots, d_{T_k}$ are weighted homogeneous. Moreover, it can be shown that $A, B, T_2, \ldots, T_k$ are also weighted homogeneous using properties of weighted homogeneous ideals given in the next section, where $d_A\tilde{a} - A, d_B\tilde{b} - B, d_{T_2}t_2 - T_2, \ldots, d_{T_k}t_k - T_k$ shall belong to a weighted homogeneous ideal derived from algebraic relations among $a, b, \tilde{a}, \tilde{b}, t_1, \ldots, t_k$.

On the other hand, as will be shown in Lemma 4.2, $t_2, \ldots, t_k$ are expressed as polynomials in $t_1, a, b, \tilde{a}, \tilde{b}$ over $\mathbb{Q}$ and those polynomials are very compact, that is, have fewer terms and smaller coefficients, and can be computed very easily. In more detail, the weight of the polynomial expression of t_i is i and its monomials are of form $t_1^{e_1} a^{e_2} b^{e_3} \tilde{a}^{e_4} \tilde{b}^{e_5}$ with $e_1 + 2e_2 + 3e_3 + 2e_4 + 3e_5 = i$. (See Section A.) Thus, we can modify our target formula as follows.

COROLLARY 3.8 (Modified Formula). *There are polynomials A, B in t_1, a, b, polynomials d_A, d_B in a, b, which are factors of d_{t_1}, and polynomials $H_2, \ldots, H_k$ in $t_1, \tilde{a}, \tilde{b}, a, b$ over $\mathbb{Q}$ such that*

$$\begin{cases} \tilde{a} = \dfrac{A(t_1; a, b)}{d_A(a, b)}, \tilde{b} = \dfrac{B(t_1; a, b)}{d_B(a, b)}, \\ t_2 = H_2(t_1, \tilde{a}, \tilde{b}; a, b), \ldots, t_k = H_k(t_1, \tilde{a}, \tilde{b}; a, b). \end{cases} \tag{9}$$

We can assume that all rational functions are reduced and degrees of A, B in t_1 are less than $\ell + 1$.

As alternative formulas for $\tilde{a}$ and $\tilde{b}$, we may consider the *rational univariate representation (RUR)* which was introduced by [23] and is *expected* to have a very compact shape. (It is also described in Theorem 10.18 in [20].) By our computational experiment for small primes ℓ, the degree of d_A and that of d_B become very huge compared with that of the denominator m'_{t_1}. (See Section A about the degrees.) Thus, use of RUR can produce a

concise formula which can be computed much easier than Shape Form formula. We show the following by using a *typical* argument for RUR.

THEOREM 3.9 (RUR Formula). *There are polynomials $\hat{A}$, $\hat{B}$ in t_1, a, b over $\mathbb{Q}$ such that the degree of $\hat{A}$ and that of $\hat{B}$ in t_1 are less than $\ell + 1$ and*

$$\tilde{a} = \frac{\hat{A}(t_1; a, b)}{m'_{t_1}(t_1; a, b)}, \quad \tilde{b} = \frac{\hat{B}(t_1; a, b)}{m'_{t_1}(t_1; a, b)}, \tag{10}$$

where $m'_{t_1}(t_1; a, b)$ denotes the derivative of $m_{t_1}(t_1; a, b)$ in t_1.

Proof. We show the formula only for $\tilde{a}$, since that for $\tilde{b}$ can be shown in the same manner. Consider all roots $\tau_1, \ldots, \tau_{\ell+1}$ of m_{t_1} in the algebraic closure $\overline{\mathbb{Q}(a, b)}$. Then, as $\tilde{a}$ is expressed as a rational function in t_1 over $\mathbb{Q}(a, b)$, each τ_i determines the value of $\tilde{a}$ which we denote by $\tilde{a}(\tau_i)$.

Now we set the following polynomial in a newly introduced variable z over $\overline{\mathbb{Q}(a, b)}$;

$$\hat{A}(z) = \sum_{i=1}^{\ell+1} \tilde{a}(\tau_i) \prod_{j \neq i} (z - \tau_j) .$$

We show that $\hat{A}(z)$ is a polynomial over $\mathbb{Q}[a, b]$. First it can be shown easily that each coefficient is stable under the action of the Galois group of m_{t_1} and therefore it belongs to $\mathbb{Q}(a, b)$. Also, since each coefficient is calculated by additions and multiplications of integral elements $\tilde{a}(\tau_1), \ldots, \tilde{a}(\tau_{\ell+1})$ and $\tau_1, \ldots, \tau_{\ell+1}$, it is also an integral element over $\mathbb{Q}[a, b]$. Thus, it should belong to $\mathbb{Q}[a, b]$. Moreover, its degree in z is less than $\ell + 1$. By easy calculation, for each τ_i, we have

$$\frac{\hat{A}(\tau_i)}{m'_{t_1}(\tau_i)} = \frac{\tilde{a}(\tau_i) \prod_{j \neq i} (\tau_i - \tau_j)}{\prod_{j \neq i} (\tau_i - \tau_j)} = \tilde{a}(\tau_i) .$$

□

REMARK 3.10. Since the leading coefficient of ψ_ℓ is ℓ, $\ell x(P)$ is integral over $\mathbb{Z}[a, b]$ for $P \in E[\ell]$. This implies that ℓt_1 is also integral over $\mathbb{Z}[a, b]$ and $m_{\ell t_1}$ belongs to $\mathbb{Z}[a, b]$. Thus, m_{t_1} belongs to $\frac{1}{\ell^{\ell+1}}\mathbb{Z}[a, b, t_1]$. In [6], it is shown that m_{t_1} belongs to $\mathbb{Z}[a, b, t_1]$ for every $\ell > 3$ by using analytic arguments. Moreover, in our computation, it is examined that $\tilde{A}$, $\tilde{B}$ also belong to $\mathbb{Z}[a, b, t_1]$.

Finally in this subsection, we discuss how the formulas can give the correct isogeny for specified values a and b. Consider arbitrary values α, β in $\mathbb{Q}$ such that $4\alpha^3 + 27\beta^2 \neq 0$ and $m_{t_1}(t_1; \alpha, \beta)$ is square free over $\mathbb{Q}$. Then, for any root τ of $m_{t_1}(t_1; \alpha, \beta)$, we can compute the values for $\tilde{a}, \tilde{b}, t_2, \ldots, t_k$ by substituting a, b, t_1 with α, β, τ in our formulas. We write $\tilde{\alpha}, \tilde{\beta}, \tau_2, \ldots, \tau_k$ for those values, respectively. By using those values, we can express $F_\ell(x)$, $D_\ell(x)$ and $N_\ell(x)$ explicitly. Here we write them by $F_\ell(x; \alpha, \beta, \tau)$, $D_\ell(x; \alpha, \beta, \tau)$ and $N_\ell(x; \alpha, \beta, \tau)$.

PROPOSITION 3.11 (Valid Formulas by Substitution). *Let α, β are rational numbers such that $4\alpha^3 + 27\beta^2 \neq 0$ and $m_{t_1}(t_1; \alpha, \beta)$ is square free over $\mathbb{Q}$. Also let τ be*

a root of $m_{t_1}(t_1; \alpha, \beta)$. *Then, the computed map* $\left(\frac{N_\ell(x;\alpha,\beta,\tau)}{D_\ell(x;\alpha,\beta,\tau)}\right)$, $y\left(\frac{N_\ell(x;\alpha,\beta,\tau)}{D_\ell(x;\alpha,\beta,\tau)}\right)'$ *is the correct isogeny from* $E(\alpha, \beta)$ *to* $E(\tilde{\alpha}, \tilde{\beta})$.

Proof. We show the statement for Shape Form formula. We note that RUR formula outputs the same value as Shape Form formula. First we prove that $\left(\frac{N_\ell(x;\alpha,\beta,\tau)}{D_\ell(x;\alpha,\beta,\tau)}\right)$, $y\left(\frac{N_\ell(x;\alpha,\beta,\tau)}{D_\ell(x;\alpha,\beta,\tau)}\right)'$ satisfies the equation $y^2 = x^3 + \tilde{\alpha}x + \tilde{\beta}$. This algebraic constraint can be reformulated in the following equation;

$$(x^3 + ax + b)(N_\ell(x)'F_\ell(x) - 2N_\ell(x)F_\ell(x)')^2 - N_\ell(x)^3 - \tilde{a}N_\ell(x)F_\ell(x)^4 - \tilde{b}F_\ell(x)^6 = 0\,. \tag{11}$$

(See Section 4.1 for details.) As Shape Form formula corresponds to the correct isogeny over $\mathbb{Q}(a, b)$, Equation (11) holds in $\mathbb{Q}(a, b)[t_1]/\langle m_{t_1}(t_1; a, b)\rangle$, where $\tilde{a}, \tilde{b}, t_2, \ldots, t_k$ are expressed as polynomials in t_1 modulo $m_{t_1}(t_1; a, b)$ over $\mathbb{Q}(a, b)$. Then the left hand side of Equation (11) is a rational function in t_1, a, b and its denominator is a product of factors of the discriminant $\mathrm{disc}(m_{t_1})$. Letting $\mathcal{N}(t_1, a, b)$ be its numerator in $\mathbb{Q}[t_1, a, b]$, we have

$$\mathcal{N}(t_1, a, b) \equiv 0 \pmod{m_{t_1}(t_1; a, b)} \text{ in } \mathbb{Q}[t_1, a, b]\,,$$

and there exists a polynomial $\mathcal{M}(t_1, a, b)$ in $\mathbb{Q}[t_1, a, b]$ such that

$$\mathcal{N}(t_1, a, b) = \mathcal{M}(t_1, a, b) \times m_{t_1}(t_1; a, b)\,.$$

Thus, for any value α, β for a, b and any root τ of $m_{t_1}(t_1; \alpha, \beta)$, as $\mathrm{disc}(m_{t_1})(\alpha, \beta) \neq 0$, all values for $\tilde{a}, \tilde{b}, t_2, \ldots, t_k$ can be determined and $\mathcal{N}(t_1, a, b)$ vanishes at (τ, α, β).

In a similar manner, we can show that $F_\ell(x; \alpha, \beta, \tau)$ is a factor of $\psi_\ell(x; \alpha, \beta)$ by the divisibility of $\psi_\ell(x; a, b)$ by $F_\ell(x; a, b, t_1)$ in $\mathbb{Q}(a, b)[t_1]/\langle m_{t_1}(t_1; a, b)\rangle$. That is, as $F_\ell(x; a, b, t_1)$ is a monic polynomial in x over $\mathbb{Q}(a, b)[t_1]$, there is a polynomial $H(x; a, b, t_1)$ in x over $\mathbb{Q}(a, b)[t_1]$ such that

$$\psi_\ell(x; a, b) - F_\ell(x; a, b, t_1)H(x; a, b, t_1) \equiv 0 \pmod{m_{t_1}(t_1; a, b)}\,.$$

Since the common denominator of coefficients of $F_\ell(x; a, b, t_1)$ is a product of factors of $\mathrm{disc}(m_{t_1})$ and $\mathrm{disc}(m_{t_1})(\alpha, \beta) \neq 0$, the congruence also holds for $\psi_\ell(x; \alpha, \beta)$ and $F_\ell(x; \alpha, \beta, \tau)$ and thus each root of $F_\ell(x; \alpha, \beta, \tau)$ is also a root of $\psi_\ell(x; \alpha, \beta)$ and so it is the x-coordinate of a point in $E[\ell]$.

Next we show that all roots of $F_\ell(x; \alpha, \beta, \tau)$ correspond to a subgroup. To prove it, we show that the x-coordinate of the i-th multiple of each point in $E[\ell]$ whose x-coordinate is a root of $F_\ell(x; a, b, t_1)$ is still a root of $F_\ell(x; a, b, t_1)$ for each positive integer i. This condition can be translated to the following algebraic condition:

$$\begin{aligned}\mathrm{resultant}_x\left(\psi_i^2(x; a, b)(y - x) + \psi_{i-1}(x; a, b)\psi_{i+1}(x; a, b),\, F_\ell(x; a, b, t_1)\right)\\ \equiv C\,F_\ell(y; a, b, t_1) \pmod{m_{t_1}(t_1; a, b)}\,,\end{aligned}$$

where $C \neq 0$ in $\mathbb{Q}(a, b)[t_1]/\langle m_{t_1}\rangle$, as $C \equiv \prod_{\gamma;\, F_\ell(\gamma)=0} \psi_i^2(\gamma; a, b)$. Then this equation also holds for $F_\ell(x; \alpha, \beta, \tau)$ and $m_{t_1}(x; \alpha, \beta)$, as the denominators never vanish at $(a, b) = (\alpha, \beta)$ by using the fact $\mathrm{disc}(m_{t_1})(\alpha, \beta) \neq 0$.

Finally, by Vélu's formula, $E(\tilde{\alpha}, \tilde{\beta})$ can be proved to be non-singular (See Lemma 12.17 in [30].) and the computed rational map is the correct isogeny. □

REMARK 3.12 (Formulas over $\mathbb{F}_p$ by Projection). Let p be an odd prime number sufficiently larger than ℓ, and consider the projection φ_p from $\mathbb{Z}_{(p)} = \{\frac{n}{m} \mid n, m \in \mathbb{Z},\ p \nmid m\}$ to the finite field $\mathbb{F}_p$ of order p. The projection φ_p can be extended naturally to polynomials over $\mathbb{Z}_{(p)}$. Then the image $\varphi_p(m_{t_1})$ does not vanish. Suppose that the image $\varphi_p(d_{t_1})$ does not vanish and all rational functions $\frac{T_i}{d_{T_2}}, \ldots, \frac{T_k}{d_{T_k}}$, $\frac{A}{d_A}$ and $\frac{B}{d_B}$ belong to $\mathbb{Z}_{(p)}(a, b)[t_1]$. Then, by the projection φ_p, all rational functions in Formula (8) can be projected to their counterparts over $\mathbb{F}_p$ which give the symbolic formula of the isogeny over $\mathbb{F}_p$. This can be examined by using ideal theoretical arguments given in the next section. Moreover, Proposition 3.11 holds for values α, β for a, b over $\mathbb{F}_p$. As to the representation of each t_i, $i > 1$, it will be shown later in Lemma 4.2 that t_i is expressed as a polynomial H_i in $a, b, \tilde{a}, \tilde{b}, t_1$ over $\mathbb{Q}$ and the common denominator of its coefficients is not divisible by any prime larger than ℓ. This implies that we have symbolic formulas of the isogeny of degree ℓ over $\mathbb{F}_p$ simply by the projection when a prime p is greater than ℓ.

4. Ideals Derived from Vélu's Formula

In this section, we consider ideals derived form Vélu's formula and analyze their properties related our symbolic formulas discussed in the previous section. We show, with help of symbolic and algebraic computation, that each zero of the ideal $I_\ell^e : 4\tilde{a}^3 + 27\tilde{b}^2$ gives an isogeny from the curve $E(a, b)$ to that $E(\tilde{a}, \tilde{b})$, where I_ℓ^e is the ideal in $K(a, b)[t_1, \tilde{a}, \tilde{b}]$ generated by algebraic constraints derived from Vélu's formula. (See Proposition 4.6.) Then, by Proposition 3.11, each zeros of the ideal I_ℓ also gives an isogeny, if it annihilates neither $D = 4a^3 + 27b^2$ nor $\tilde{D} = 4\tilde{a}^3 + 27\tilde{b}^2$ but keep the minimal polynomial m_{t_1} square-free. Thus, Vélu's formula can be considered as *a generic formula* for isogenies in algebraic sense. We first handle $a, b, \tilde{a}, \tilde{b}, t_1, \ldots, t_k$ as variables in the formulas in Proposition 2.1 and focus on the ring of multivariate polynomials $\mathcal{R}_0 = K[a, b, \tilde{a}, \tilde{b}, t_1, \ldots, t_k]$, where K is an arbitrary computable field with characteristic 0 or sufficiently large characteristic. Next, we reduce variables and handle only $a, b, \tilde{a}, \tilde{b}, t_1$ and focus on the ring of multivariate polynomials $\mathcal{R} = K[a, b, \tilde{a}, \tilde{b}, t_1]$.

4.1. Generating Ideals Corresponding to Vélu's Formula

Here we give an explicit system of algebraic equations derived from Vélu's formula. Since $\phi(x, y) \in \widetilde{E}$ can be rewritten as the formula (1) for any $(x, y) \in E$, the equation

$$\left(y\left(\frac{N_\ell(x)}{D_\ell(x)}\right)'\right)^2 - \left(\frac{N_\ell(x)}{D_\ell(x)}\right)^3 - \tilde{a}\left(\frac{N_\ell(x)}{D_\ell(x)}\right) - \tilde{b} = 0 \tag{12}$$

is satisfied. Since $y^2 = x^3 + ax + b$ for $(x, y) \in E$, Equation (12) depends on the unique variable x:

$$(x^3+ax+b)\left(\frac{N_\ell(x)'D_\ell(x) - N_\ell(x)D_\ell(x)'}{D_\ell(x)^2}\right)^2 - \left(\frac{N_\ell(x)}{D_\ell(x)}\right)^3 - \tilde{a}\left(\frac{N_\ell(x)}{D_\ell(x)}\right) - \tilde{b} = 0\,. \tag{13}$$

As $D_\ell(x) = F_\ell(x)^2$, we have the following by eliminating a factor $F_\ell(x)^2$ from the numerator of Equation (13):

$$(x^3 + ax + b)(N_\ell(x)' F_\ell(x) - 2N_\ell(x)F_\ell(x)')^2 - N_\ell(x)^3 - \tilde{a}N_\ell(x)F_\ell(x)^4 - \tilde{b}F_\ell(x)^6 = 0\,, \tag{14}$$

where $N_\ell(x)$ is expressed by $F_\ell(x)$ and its derivatives in Equation (5). Using the weights in Remark 2.2 and letting *weights* of $\tilde{a}, \tilde{b}$ be $2, 3$, respectively, the polynomial of the left hand side of Equation (14) is homogeneous of weight $6k + 3$, where the weights of $F_\ell(x)$, $F'_\ell(x)$, $N_\ell(x)$, and $N'_\ell(x)$ are $k, k-1, 2k+1$ and $2k$, respectively. Then, from Equation (14), we have

$$f_{6k+3}x^{6k+3} + f_{6k+2}x^{6k+2} + f_{6k+1}x^{6k+1} + \cdots + f_0 = 0\,, \tag{15}$$

where each f_i is a polynomial in $t_1, \ldots, t_k, a, b, \tilde{a}, \tilde{b}$ over K.

Now we consider the ideal I^0_ℓ generated by all f_i's in $\mathcal{R}_0 = K[a, b, \tilde{a}, \tilde{b}, t_1, \ldots, t_k]$;

$$I^0_\ell = \langle f_0, \ldots, f_{6k+3}\rangle_{\mathcal{R}_0}$$

Since each isogeny from $E(a, b)$ gives a zero of I^0_ℓ over $\overline{K}$, I^0_ℓ is non-trivial. Conversely, each zero $(\alpha, \beta, \tilde{\alpha}, \tilde{\beta}, \tau_1, \ldots, \tau_k)$ of I^0_ℓ over $\overline{K}$ gives a rational map from $E(\alpha, \beta)$ to $E(\tilde{\alpha}, \tilde{\beta})$ and if both $E(\alpha, \beta)$ and $E(\tilde{\alpha}, \tilde{\beta})$ are elliptic curves, the rational map is an isogeny. (See Remark 2.3 and Proposition 4.6.)

REMARK 4.1. As the polynomial of the left hand side of Equation (14) is weighted homogeneous, all f_i's are also weighted homogeneous. As the weight of f_{6k+3} is 0, we can show $f_{6k+3} = 0$. Moreover, as the weight of f_{6k+2} is 1 and t_1 is the unique variable of weight 1, we can also show $f_{6k+2} = 0$.

Counting weights of terms appearing in f_i's, we have the following.

LEMMA 4.2. *For each integer i, $2 \le i \le k$, the coefficient polynomial f_{6k+3-i} is of weight i and contains a term ct_i, where c is a non-zero element of K. Moreover, from the equation $f_{6k+3-i} = 0$, t_i is expressed as a polynomial in $a, b, \tilde{a}, \tilde{b}, t_1$ over K. The common denominator of its coefficients as rational numbers is not divisible by any prime number greater than ℓ.*

Proof. We consider how t_i can appear in f_{6k+3-i} for $2 \le i \le k$. As f_{6k+3-i} is 0 or of weight i, t_i may appear in f_{6k+1-i} as ct_i for some constant c in K. By the definition (4), t_i appears only in the coefficient of x^{k-i} in $F_\ell(x)$. From Equation (5), it follows that, in $N_\ell(x)$, t_i does not appear in any coefficient of x^{2k+1-j} for $j < i$ and t_i appears in the coefficient of x^{2k+1-i} with constant multiple $-4i^2+2i+2$. Also, as the leading coefficient of N_ℓ is 1, t_i can appear in the coefficient of x^{6k+3-i} in N_ℓ^3 with constant multiple $3 \times (-4i^2 + 2i + 2)$. In the same manner, we can show that in $(x^3 + ax + b)(N_\ell(x)' F_\ell(x) - 2N_\ell(x)F_\ell(x)')^2$, t_i appears in the coefficient of x^{6k+3-i} with constant multiple $8i^3 - 12i^2 + 4i + 6$. On the other hand, as the weight of $\tilde{a}$ is 2 and that of $\tilde{b}$ is 3, t_i can appear in the coefficient of x^{6k+3-i} in neither the term $\tilde{a}N_\ell(x)F_\ell(x)^4$ nor $\tilde{b}F_\ell(x)^6$.

Thus, t_i can appear in the coefficient of x^{6k+3-i} in the left hand side of Equation (14) with non-zero constant multiple $C_i = 8i^3 - 2i = (2i-1)(2i+1)2i$. (We note that the constant does not depend on k.) Therefore, for $i \ge 2$, it follows that $C_i \ne 0$.

Now, f_{6k+3-i} can be written as

$$f_{6k+3-i} = C_i t_i - g_i(a, b, \tilde{a}, \tilde{b}, t_1, t_2, \ldots, t_{i-1}),$$

where $g_i(a, b, \tilde{a}, \tilde{b}, t_1, t_2, \ldots, t_{i-1})$ is a polynomial in $a, b, \tilde{a}, \tilde{b}, t_1, t_2, \ldots, t_{i-1}$ over K, and thus, by using *recursive substitution*

$$t_i \leftarrow \frac{g_i(a, b, \tilde{a}, \tilde{b}, t_1, t_2, \ldots, t_{i-1})}{C_i}$$

(which is equivalent to *remainder (polynomial division)* computations by monic polynomials $t_i - \frac{g_i(a,b,\tilde{a},\tilde{b},t_1,t_2,\ldots,t_{i-1})}{C_i}$), it can be shown that the ideal I_ℓ^0 has a polynomial h_i of the following form;

$$h_i = t_i - H_i(a, b, \tilde{a}, \tilde{b}, t_1),$$

where $H_i(a, b, \tilde{a}, \tilde{b}, t_1)$ is a polynomial in $a, b, \tilde{a}, \tilde{b}, t_1$ over K. Since $C_i = (2i - 1)(2i + 1)2i$ for $2 \le i \le k = \frac{\ell-1}{2}$, it can be shown directly that the common denominator of coefficients of H_i is not divisible by any prime greater than ℓ. □

EXAMPLE 4.3. We give polynomial expressions of t_i for several smaller ℓ.
$\ell = 5$:

$$t_2 = \frac{19a + \tilde{a} + 30t_1^2}{2^2 3^1 5^1}.$$

$\ell = 7$:

$$t_2 = \frac{29a + \tilde{a} + 30t_1^2}{2^2 3^1 5^1}, \quad t_3 = \frac{119t_1 a + 166b + 7t_1\tilde{a} + 2\tilde{b} + 70t_1^3}{2^2 3^1 5^1 7^1}.$$

The set $\{t_2 = H_2, \ldots, t_k = H_k\}$ in the proof of Lemma 4.2 is essentially the same as the set of relations among $t_1, \ldots, t_k, a, b, \tilde{a}, \tilde{b}$ given in [24] which was derived from analytic arguments. Applying substitution t_i with h_i to other f_{6k+3-i} for $i > k$, we can make them polynomials in $t_1, a, b, \tilde{a}, \tilde{b}$ over K and we denote it by $\tilde{f}_{6k+3-i}$. Thus, for finding zeros of I_ℓ^0, we need only to consider the ideal I_ℓ in $\mathcal{R}$ generated by all such polynomials $\tilde{f}_{5k+2}, \ldots, \tilde{f}_0$. Letting $G_0 = \{\tilde{f}_{5k+2}, \ldots, \tilde{f}_0\}$,

$$I_\ell = \langle G_0 \rangle_{\mathcal{R}} = \langle \tilde{f}_{5k+2}, \ldots, \tilde{f}_0 \rangle_{\mathcal{R}}.$$

As a notation, we let $(I_\ell^0)^e$ the extension of I_ℓ^0 over $K(a, b)[\tilde{a}, \tilde{b}, t_1, \ldots, t_k]$ and I_ℓ^e that of I_ℓ over $K(a, b)[\tilde{a}, \tilde{b}, t_1]$.

LEMMA 4.4. *I_ℓ is the elimination ideal of I_ℓ^0, that is $I_\ell = I_\ell^0 \cap \mathcal{R}$. Moreover, each zero of I_ℓ can be extended uniquely to a zero of I_ℓ^0. These properties also hold for I_ℓ^e and $(I_\ell^0)^e$.*

Proof. Let $H = \{h_2, \ldots, h_k\}$. First we show that $G_0 \cup H$ also generates the ideal I_ℓ^0. This is because each h_i is the remainder of f_{6k+3-i} by $h_2, \ldots, h_{i-1}$ up to constant multiple and each $\tilde{f}_i$ is also the remainder of f_i by $h_2, \ldots, h_k$ up to a constant multiple. Thus, the ideal generated by $G_0 \cup H$ contains I_ℓ^0. Conversely, G_0 and H are constructed by polynomial divisions from $\{f_{6k+1}, \ldots, f_0\}$, it is clear that I_ℓ^0 contains $G_0 \cup H$ and the ideal generated by them.

Next we show that I_ℓ coincides with $I_\ell^0 \cap \mathcal{R}$. As G_0 is contained in $I_\ell^0 \cap \mathcal{R}$, I_ℓ is contained in $I_\ell^0 \cap \mathcal{R}$. Thus, it suffices to show that for each g in $I_\ell^0 \cap \mathcal{R}$, g belongs to I_ℓ. As g belongs to I_ℓ^0, there are polynomials u_i in $\mathcal{R}_0$ such that $g = \sum_{i=0}^{6k+1} u_i f_i$. Since $\tilde{f}_i$ is the remainder of f_i by H and $f_{6k+1}, \ldots, f_{5k+3}$ are expressed as linear sums on H over $\mathcal{R}_0$, letting $\tilde{u}_i$ be the remainder of u_i by H, we have

$$g = \sum_{i=0}^{6k+1} u_i f_i = \sum_{i=0}^{5k+2} \tilde{u}_i \tilde{f}_i + \sum_{i=2}^{k} v_i h_i \,,$$

for some $v_i \in \mathcal{R}_0$. Then $\tilde{u}_i$ belongs to $\mathcal{R}$ and $\sum_{i=0}^{5k+2} \tilde{u}_i \tilde{f}_i$ belongs to $I_\ell \subset \mathcal{R}$. Thus, as g belongs to $\mathcal{R}$, $\sum_{i=2}^{k} v_i h_i$ also belongs to $\mathcal{R}$.

On the other hand, H forms a Gröbner basis of the ideal in $\mathcal{R}_0$ generated by itself with respect to a *block (or product) monomial ordering* $\prec$ such that $\{a, b, \tilde{a}, \tilde{b}, t_1\} \ll \{t_2, \ldots, t_k\}$, since their leading monomials are relatively prime. (See Proposition 4 and Exercise 3 in Chapter 2.9 in [8], and see also [11, 8] for monomial orderings.) Seeing their leading monomials $t_2, \ldots, t_k$, the ideal generated by H does not contain non-zero element in $\mathcal{R} = k[a, b, \tilde{a}, \tilde{b}, t_1]$. This means that $\sum_{i=2}^{k} v_i h_i = 0$ and g belongs to I_ℓ.

Finally we show that each zero of I_ℓ can be extended to a zero of I_ℓ^0. For each $h_i = t_i - H_i(a, b, \tilde{a}, \tilde{b}, t_1)$ in I_ℓ^0, its leading coefficient never vanish at any zero of I_ℓ. Thus, by the extension theorem (see Theorem 3 in Chapter 3.5 in [8]), each zero of I_ℓ can be extended to a zero of I_ℓ^0. Also, the value of t_i is uniquely determined by the values of $a, b, \tilde{a}, \tilde{b}, t_1$. □

4.2. Structure of Ideals

Now we analyze the structure of the ideal I_ℓ in $\mathcal{R}$. Let $D(x, y) = 4x^3 + 27y^2$, $D = D(a, b) = 4a^3 + 27b^2$ and $\tilde{D} = D(\tilde{a}, \tilde{b}) = 4\tilde{a}^3 + 27\tilde{b}^2$.

REMARK 4.5. As Vélu's formula is constructed from a subgroup S of order ℓ, it is automatically proved that the constructed map is a *morphism* and $\tilde{E} = E(\tilde{a}, \tilde{b})$ is also an elliptic curve. (See Lemma 12.17 in [30]). But, in our case, for each zero $(\alpha, \beta, \tilde{\alpha}, \tilde{\beta}, \tau)$ of I_ℓ, we do not know about the algebraic *structure* of the kernel of computed polynomial F_ℓ. Thus, even if $D(\alpha, \beta) \neq 0$, it is difficult to predict $D(\tilde{\alpha}, \tilde{\beta}) \neq 0$. Also, we have to check whether the map is a morphism. This implies that we have to consider special ideals based on *saturation and extension* for eliminating cases $D = 0$ and $\tilde{D} = 0$ to make $E(\alpha, \beta)$ and $E(\tilde{\alpha}, \tilde{\beta})$ elliptic curves.

On the other hand, from our experiment for smaller primes ℓ, the condition $D \neq 0$ seems enough to obtain our formulas, because $D(\tilde{\alpha}, \tilde{\beta})$ cannot vanish for every zero $(\alpha, \beta, \tilde{\alpha}, \tilde{\beta}, \tau)$ of I_ℓ with $D(\alpha, \beta) \neq 0$. Therefore, we mainly consider the ideal $I_\ell : D^\infty$ for our experiment. See Conjecture for the detail.

Next we consider the ideal $\hat{I}_\ell$ generated by I_ℓ and $u\tilde{D} - 1$ in $K[a, b, \tilde{a}, \tilde{b}, t_1, u]$, where u is a new variable, its extension $\hat{I}_\ell^e$ of $\hat{I}_\ell$ in $K(a, b)[\tilde{a}, \tilde{b}, t_1, u]$ and its elimination ideal $\hat{I}_\ell^e \cap K(a, b)[\tilde{a}, \tilde{b}, t_1]$. $\hat{I}_\ell^e$ is also generated by I_ℓ^e and $u\tilde{D} - 1$. Then, $\hat{I}_\ell^e \cap K(a, b)[\tilde{a}, \tilde{b}, t_1]$ coincides with the *saturation* $I_\ell^e : \tilde{D}^\infty$ of I_ℓ^e with respect to $\tilde{D}$. Now we can show the following.

PROPOSITION 4.6. *$\hat{I}_\ell^e$ is 0-dimensional in $K(a,b)[\tilde{a},\tilde{b},t_1,u]$ and it has exactly $\ell+1$ distinct zeros over the algebraic closure $\overline{K(a,b)}$, each of which corresponds to a distinct isogeny of degree ℓ from $E(a,b)$. Moreover, $I_\ell^e : \tilde{D}^\infty$ is also 0-dimensional in $K(a,b)[\tilde{a},\tilde{b},t_1]$ and it contains exactly $\ell+1$ distinct zeros which correspond to zeros of $\hat{I}_\ell^e$.*

Proof. We first show that any zero $(\tilde{\alpha},\tilde{\beta},\tau,\upsilon)$ of $\hat{I}_\ell^e$ over the algebraic closure $\overline{K(a,b)}$ corresponds to an isogeny from $E=E(a,b)$ to $E(\tilde{\alpha},\tilde{\beta})$. (Here, $\tilde{\alpha}$, $\tilde{\beta}$, τ and υ correspond to $\tilde{a}$, $\tilde{b}$, t_1 and u, respectively.) We note that for such zero $(\tilde{\alpha},\tilde{\beta},\tau,\upsilon)$, $(\tilde{\alpha},\tilde{\beta},\tau)$ is a zero of I_ℓ^e and $\tilde{D}=4\tilde{\alpha}^3+27\tilde{\beta}\neq 0$. By Lemma 4.4 $(\tilde{\alpha},\tilde{\beta},\tau)$ gives a zero of $(I_\ell^0)^e$.

As we are considering all computation over $K(a,b)$, it follows that $D=4a^3+27b^2\neq 0$. Also, by substituting $\tilde{a},\tilde{b},t_1,u$ with $\tilde{\alpha},\tilde{\beta},\tau,\upsilon$, we have $\tilde{D}=4\tilde{\alpha}^3+27\tilde{\beta}^2\neq 0$ and $\tilde{E}=E(\tilde{\alpha},\tilde{\beta})$ is an elliptic curve over $\overline{K(a,b)}$. Now we can construct the rational map ϕ from $E(a,b)$ to $E(\tilde{\alpha},\tilde{\beta})$ as follows:

$$\phi : E(a,b)\ni(x,y)\mapsto\left(\frac{N_\ell(x;\tilde{\alpha},\tilde{\beta},\tau)}{F_\ell^2(x;\tilde{\alpha},\tilde{\beta},\tau)},\, y\left(\frac{N_\ell(x;\tilde{\alpha},\tilde{\beta},\tau)}{F_\ell^2(x;\tilde{\alpha},\tilde{\beta},\tau)}\right)'\right)\in E(\tilde{\alpha},\tilde{\beta})\,,$$

where $F_\ell(x;\tilde{\alpha},\tilde{\beta},\tau)$ and $N_\ell(x;\tilde{\alpha},\tilde{\beta},\tau)$ are determined by the values $\tilde{\alpha}$, $\tilde{\beta}$, τ. (See Proposition 3.11 and Lemma 4.4.) As shown in Remark 2.3, by using properties of F_ℓ, D_ℓ, N_ℓ, ϕ maps the point at infinity of E to that of $\tilde{E}$. Thus, to confirm that the map ϕ is an isogeny of degree ℓ, we show that it maps P to the point at infinity of $\tilde{E}$ for each point P on E such that $x(P)$ is a root of $F_\ell(x;\tilde{\alpha},\tilde{\beta},\tau)$ and $F_\ell(x;\tilde{\alpha},\tilde{\beta},\tau)$ is square-free.

By the construction of N_ℓ, we derive the following properties. (For simplicity, we write F and N for $F_\ell(x;\tilde{\alpha},\tilde{\beta},\tau)$ and $N_\ell(x;\tilde{\alpha},\tilde{\beta},\tau)$, respectively.)

(i) If F and N have a common irreducible factor which does not divide x^3+ax+b, then it is a multiple factor of F.

This can be shown by using Equation (5) of the *construction* of N by F. Let G be a common irreducible factor of F and N, and H its cofactor of F. Then $F=GH$. By substituting F with GH in Equation (5), we have

$$4(x^3+ax+b)G'^2H^2\equiv N\equiv 0 \pmod{G}\,.$$

From this, as G is irreducible, G should divide (x^3+ax+b) or H. In the latter case, G is a multiple factor of F.

(ii) Conversely, if F have a multiple factor, then it is also a factor of N. Moreover, if F has a common factor with x^3+ax+b, then it is also a factor of N.

This can be shown in a similar manner as (i) by using Equation (5). As to a multiple factor G, by letting $F=HG^2$ and substituting it in Equation (5), we can examine that G^2 divides N. Also, for a common factor G of F and x^3+ax+b, it is clear that G divides N.

(iii) F cannot have any multiple irreducible factor except its GCD with x^3+ax+b.

Suppose that G is an irreducible factor of F with multiplicity e. Let H be the cofactor of G^e of F. Then, by combining Equations (5) and (14), we have

$$64e^2(e-1)(x^3+ax+b)^3G'^6H^4\equiv 0 \pmod{G}\,.$$

Therefore, unless G is a factor of x^3+ax+b, G should divides either G' or H. This is a contradiction.

(iv) F and x^3+ax+b have no common factor.

We can show it in the same manner as (iii). Suppose that G is an irreducible factor of F and x^3+ax+b and its multiplicity as a factor of F is e. Let H be the cofactor of G^e of F and M the cofactor of G of x^3+ax+b. (We note that x^3+ax+b is square-free over $K(a,b)$.) Then, by combining Equations (5) and (14), we have

$$4e^2(2e-1)G'^6H^4M^3 \equiv 0 \pmod{G}.$$

As G is irreducible and divides neither G', H nor M, we have a contradiction.

Combining properties (i),...,(iv), we conclude the following.

(v) F is square-free, F has no common factor with N and F has no common factor with x^3+ax+b.

We note that, as e is not greater than the degree k of F, we have $e \le k = \frac{\ell-1}{2}$. So, when $K=\mathbb{F}_p$, we have $e < \frac{p-1}{2}$ by our assumption, and $64e^2(e-1) \neq 0$ and $4e^2(2e-1) \neq 0$ in $\mathbb{F}_p$.

From the property (v), it follows that for each point P on E such that $x(P)$ is a root of $F(x)$, we have $y(P) \neq 0$ and $N(x(P)) \neq 0$. Then, the map written in a projective form

$$\phi([x,y,z]) = \left[F^*N^*,\, y(N'F-2NF')^*,\, z(F^*)^3\right]$$

transform $[x(P), y(P), 1]$ to $[0, -2y(P)N(x(P))F'(x(P)), 0] = [0,1,0]$, as $y(P) \neq 0$, $F'(x(P)) \neq 0$ and $N(x(P)) \neq 0$. Thus we have shown that ϕ is an isogeny from E to $\tilde{E}$. Moreover, as F is square-free, the number of points in the kernel of ϕ (including the point at infinity) is ℓ, which implies that the kernel of ϕ is a subgroup of order ℓ of the ℓ-torsion subgroup $E[\ell]$.

On the other hand, there are $\ell+1$ subgroups of order ℓ in E, and their points are all algebraic over $K(a,b)$. (See Lemma 2.6.) Thus, from each subgroup S, we have algebraic elements $\tilde{\alpha}_S, \tilde{\beta}_S, \tau_S$ that satisfy all $\tilde{f}_{6k+3-i}$ in the previous subsection. Thus, $(\tilde{\alpha}_S, \tilde{\beta}_S, \tau_S, \upsilon_S)$, where $\upsilon_S = \frac{1}{\tilde{D}(\tilde{\alpha}_S, \tilde{\beta}_S)}$, is a zero of $\hat{I}_\ell^e$. Hence we conclude that the number of distinct zeros is $\ell+1$ and $\hat{I}^e$ is 0-dimensional in $K(a,b)[\tilde{a},\tilde{b},t_1]$.

As to $I_\ell^e : \tilde{D}^\infty$, since it is the elimination ideal of $\hat{I}_\ell^e$ which is 0-dimensional, it is also 0-dimensional. Also, by the closure theorem, it contains the projected zero $(\tilde{\alpha}_S, \tilde{\beta}_S, \tau_S)$ of $(\tilde{\alpha}_S, \tilde{\beta}_S, \tau_S, \upsilon_S)$ for all subgroups S. (See Theorem 3 in Chapter 3.2 in [8]).

Meanwhile, since the 0-dimensionality of $\hat{I}_\ell^e$ implies that there is a polynomial whose leading term is a power of u, all zeros of its elimination ideal $I_\ell^e : \tilde{D}^\infty$ can be extended to a zero of $\hat{I}_\ell^e$ by the extension theorem. Also, as υ is determined uniquely from $\tilde{\alpha}$ and $\tilde{\beta}$, it follows directly that there is one to one correspondence between distinct zeros of $\hat{I}_\ell^e$ and those of $I_\ell^e : \tilde{D}^\infty$. □

When $K=\mathbb{Q}$, by using Lemma 3.3, we can show the primariness of $I_\ell^e : \tilde{D}^\infty$ as follows. Let $z_1 = (\tilde{\alpha}_1, \tilde{\beta}_1, \tau_1), \ldots, z_{\ell+1} = (\tilde{\alpha}_{\ell+1}, \tilde{\beta}_{\ell+1}, \tau_{\ell+1})$ be the distinct zeros of $I_\ell^e : \tilde{D}^\infty$. Then, for each z_i, there is a unique extended zero z_i^0 of $(I_\ell^0)^e$ that gives a factor, say

$F^{(i)}(x)$, of $\psi_\ell(x)$. Since $\psi_\ell(x; a, b)$ is irreducible and its Galois group is isomorphic to $GL(2, \ell)/Z_2$, all $F^{(1)}(x), \ldots, F^{(\ell+1)}$ are conjugate to each other by the action of the Galois group. This implies that $z_1, \ldots, z_{\ell+1}$ are conjugate by the Galois group action. Hence the variety $\{z_1, \ldots, z_{\ell+1}\}$ is irreducible over $\mathbb{Q}(a, b)$ and $\sqrt{I_\ell^e : \tilde{D}^\infty}$ is a prime (maximal) ideal, that is, $I_\ell^e : \tilde{D}^\infty$ consists of one primary component. We note that $\sqrt{I_\ell^e : \tilde{D}^\infty} = \sqrt{I_\ell^e} : \tilde{D}$. (See Proposition 9 in Chapter 4.4 in [8].)

THEOREM 4.7. (1) *The extension ideal* $I_\ell^e : \tilde{D}^\infty$ *of* $K(a,b)[\tilde{a},\tilde{b},t_1]$ *is 0-dimensional, and the linear dimension of the residue class ring* $\dfrac{K(a, b)[\tilde{a}, \tilde{b}, t_1]}{\sqrt{I_\ell^e} : \tilde{D}}$ *is* $\ell + 1$.

(2) *The contraction ideal* $(I_\ell^e : \tilde{D}^\infty)^c = I_\ell^{ec} : \tilde{D}^\infty$ *is 2-dimensional.*

(3) *When* $K = \mathbb{Q}$, $\sqrt{I_\ell^e} : \tilde{D}$ *is a maximal ideal and* $I_\ell^e : \tilde{D}^\infty$ *and* $I_\ell^{ec} : \tilde{D}^\infty$ *are primary ideals. We may call* $I_\ell^{ec} : \tilde{D}^\infty$ *the* generic *component of* I_ℓ *which shall give our formulas.*

REMARK 4.8. By our experiment, when $K = \mathbb{Q}$, for smaller primes ℓ, the ideal I_ℓ consists of the generic component $I_\ell^{ec} : \tilde{D}^\infty = I_\ell : D^\infty$ and other components coming from the condition that E is singular. Moreover, I_ℓ^e is *maximal*. By modular techniques, computation of Gröbner basis of $I_\ell : D^\infty$ seems to be done much efficiently compared with that of I_ℓ^e. See *Conjecture* in the next subsection.

4.3. More on Ideals and Conjecture

By Theorem 4.7, $I_\ell^e : \tilde{D}^\infty$ is 0-dimensional and has $\ell + 1$ distinct zeros all of which correspond to isogenies. Thus, for $t_1, \tilde{a}, \tilde{b}$, there exist their minimal polynomials modulo $\sqrt{I_\ell^e} : \tilde{D}$ over $K(a, b)$, and we denote them $m_{t_1}(x), m_{\tilde{a}}(x), m_{\tilde{b}}(x)$. This fact corresponds to Lemma 3.2. Moreover, as shown in Lemma 3.2, $m_{t_1}, m_{\tilde{a}}, m_{\tilde{b}}$ are polynomials over $K[a, b]$.

LEMMA 4.9. *Minimal polynomials* $m_{t_1}(x)$, $m_{\tilde{a}}(x)$ *and* $m_{\tilde{b}}(x)$ *modulo* $\sqrt{I_\ell^e} : \tilde{D}$ *are defined over* $K[a, b]$.

As a consequence of Lemma 4.9, since $m_{t_1}(t_1)$, $m_{\tilde{a}}(\tilde{a})$ and $m_{\tilde{b}}(\tilde{b})$ belong to $\mathcal{R} = K[a, b, \tilde{a}, \tilde{b}, t_1]$, we have the following.

COROLLARY 4.10. *The contraction ideal* $\sqrt{I_\ell^{ec}} : \tilde{D}$ *of* $\sqrt{I_\ell^e} : \tilde{D}$ *contains* $m_{t_1}(t_1)$, $m_{\tilde{a}}(\tilde{a})$ *and* $m_{\tilde{b}}(\tilde{b})$. *When* $K = \mathbb{Q}$, $I_\ell^{ec} : \tilde{D}^\infty$ *is a primary component of* I_ℓ *and so its associate prime contains them.*

COROLLARY 4.11. *Minimal polynomials* $m_{t_1}(t_1)$, $m_{\tilde{a}}(\tilde{a})$ *and* $m_{\tilde{b}}(\tilde{b})$ *are weighted homogeneous.*

Proof. As I_ℓ is weighted homogeneous ideal with respect to the given weights, all components and associated primes are also weighted homogeneous. Therefore, $\sqrt{I_\ell^{ec}} : \tilde{D}$ is weighted homogeneous and every homogeneous part of $m_{t_1}(t_1)$ is also belonging to $\sqrt{I_\ell^{ec}} : \tilde{D}$. By the minimality, it follows that $m_{t_1}(t_1)$ has a unique homogeneous part and so

it is weighted homogeneous. In the same manner, we can prove that $m_{\tilde{a}}(\tilde{a})$ and $m_{\tilde{b}}(\tilde{b})$ are weighted homogeneous. □

When $K = \mathbb{Q}$, as the number of zeros of $\sqrt{I_\ell^e} : \tilde{D}$ is $\ell + 1$, the residue class ring $\dfrac{\mathbb{Q}(a,b)[\tilde{a},\tilde{b},t_1]}{\sqrt{I_\ell^e} : \tilde{D}}$ is considered as an algebraic extension field of $\mathbb{Q}(a,b)$ of degree $\ell+1$. Moreover, by Lemma 3.5, t_1 is in *generic position*, that is, $m_{t_1}(x)$ has degree $\ell+1$ and $\tilde{a}, \tilde{b}$ can be expressed as polynomials in t_1 over $\mathbb{Q}(a,b)$ given in Lemma 3.6. For any zero (α, β, τ) of $I_\ell^e : \tilde{D}^\infty$, we have

$$m_{t_1}(\tau; a, b) = 0, \alpha = \frac{A(\tau; a, b)}{d_A(a,b)}, \beta = \frac{B(\tau; a, b)}{d_B(a,b)},$$

where $A(x; a, b)$, $B(x; a, b)$ are polynomials over $\mathbb{Q}[a, b]$ and $d_A(a, b)$, $d_B(a, b)$ are factors of the discriminant of m_{t_1}. (We note that degree of $A(x; a, b)$ and that of $B(x; a, b)$ in x are less than $\ell + 1$, and $\gcd(d_A(a, b), A(x; a, b)) = \gcd(d_B(a, b), B(x; a, b)) = 1$.)

Let GB be the following set:

$$GB = \left\{ m_{t_1}(t_1; a, b), \tilde{a} - \frac{A(t_1; a, b)}{d_A(a,b)}, \tilde{b} - \frac{B(t_1; a, b)}{d_B(a,b)} \right\}. \tag{16}$$

As $\sqrt{I_\ell^e} : \tilde{D}$ is radical, GB is included in $\sqrt{I_\ell^e} : \tilde{D}$ by Hilbert's Nullstellensatz. By its shape, GB forms a Gröbner basis of the ideal generated by itself. Then, comparing the linear dimensions, it follows that it also forms the reduced Gröbner basis of $\sqrt{I_\ell^e} : \tilde{D}$ with respect to a block monomial ordering $<$ such that $\{t_1\} \ll \{\tilde{a}, \tilde{b}\}$ so called in *shape form*. Also, by saturation technique for contraction ideal (see Lemma 8.91 and Proposition 8.92 in [3]) $\sqrt{I_\ell^{ec}} : \tilde{D}$ can be computed by GB as follows:

$$\sqrt{I_\ell^{ec}} : \tilde{D} = J_\ell : (d_A(a,b) d_B(a,b))^\infty, \tag{17}$$

where J_ℓ is the ideal in $\mathbb{Q}[a, b, \tilde{a}, \tilde{b}, t_1]$ generated by $m_{t_1}(t_1; a, b)$, $d_A(a,b)\tilde{a} - A(t_1; a, b)$ and $d_B(a, b)\tilde{b} - B(t_1; a, b)$. Then $d_A(a,b)\tilde{a} - A(t_1; a, b)$ and $d_B(a, b)\tilde{b} - B(t_1; a, b)$ belong to $\sqrt{I_\ell^{ec}} : \tilde{D}$. Thus, by considering homogeneous parts, we can show that they are weighted homogeneous. This implies that $A(t_1; a, b)$ and $B(t_1; a, b)$ are weighted homogeneous.

Now we propose our conjecture for making our computation practical, where another ideal $I_\ell : D^\infty$ plays an important role. As $D \in K[a, b]$, $\sqrt{I_\ell^{ec}} : \tilde{D} \supset I_\ell^{ec} : \tilde{D}^\infty \supset I_\ell^{ec} \supset I : D^\infty$

Conjecture: By our computational experiments for small primes ℓ, we set the following as our conjecture for $K = \mathbb{Q}$ and a finite field $\mathbb{F}_p$ with sufficiently large p.

- I_ℓ^e is maximal, $I_\ell^e = \sqrt{I_\ell^e} = I_\ell^e : \tilde{D}^\infty$ and $I_\ell^{ec} = \sqrt{I_\ell^{ec}} = \sqrt{I_\ell^{ec}} : \tilde{D}$.
- I_ℓ consists of one prime component I_ℓ^{ec} and others containing some powers of D. This implies $\sqrt{I_\ell^{ec}} : \tilde{D} = I_\ell : D^\infty$.

From our experiments, a Gröbner basis of the ideal $I_\ell : D^\infty$ can be computed very efficiently compared with that of I_ℓ^e. (See the next section for computational details.) Moreover, by our conjecture, $I_\ell : D^\infty$ coincides with the generic component $I_\ell^{ec} : \tilde{D}^\infty$, and we

may have very useful information from its Gröbner basis. Thus, we provide the following proposition which is useful for checking our conjecture and for constructing our formulas. Let G be the reduced Gröbner basis of $I_\ell : D^\infty$ in $K[a, b, \tilde{a}, \tilde{b}, t]$ with respect to a block monomial ordering $<$ such that $\{a, b, t_1\} \ll \{\tilde{a}, \tilde{b}\}$. Comparing the linear dimension of $\dfrac{K(a,b)[\tilde{a},\tilde{b},t_1]}{(I_\ell : D^\infty)^e}$ with that of $\dfrac{K(a,b)[\tilde{a},\tilde{b},t_1]}{\sqrt{I_\ell^e} : \tilde{D}}$, we have the following:

PROPOSITION 4.12. *If $G \cap K[t_1, a, b]$ consists of one polynomial which is irreducible in $K[t_1, a, b]$ and monic and of degree $\ell + 1$ with respect to t_1, then it coincides with the minimal polynomial $m_{t_1}(t_1; a, b)$ and t_1 is in generic position.*

Moreover, if G contains a polynomial A in $\tilde{a}, t_1, a, b$ and a polynomial B in $\tilde{b}, t_1, a, b$ such that the degree of A with respect to $\tilde{a}$ is 1 and that of B with respect to $\tilde{b}$ is 1, then $(I_\ell : D^\infty)^e$ is maximal and thus $(I_\ell : D^\infty)^e = I_\ell^e = \sqrt{I_\ell^e} = \sqrt{I_\ell^e} : \tilde{D} = J_\ell^e$. (This implies that I_ℓ^{ec} is a 2-dimensional prime ideal. We note that $(I_\ell : D^\infty) \cap K[a, b] = \{0\}$ as there is no element in G whose leading monomial belongs to $K[a, b]$.)

Finally we consider the RUR formula given in Theorem 3.9. By Hilbert's Nullstellensatz, $m'_{t_1}(t_1; a, b)\tilde{a} - \hat{A}(t_1; a, b)$ and $m'_{t_1}(t_1; a, b)\tilde{b} - \hat{B}(t_1; a, b)$ should belong to $\sqrt{I_\ell^e} : \tilde{D}$. Since the both are polynomials in $t_1, a, b, \tilde{a}, \tilde{b}$ over $\mathbb{Q}$, they belong to $(\sqrt{I_\ell^e} : \tilde{D})^c = \sqrt{I_\ell^{ec}} : \tilde{D}$. If Conjecture holds, they belong to $I_\ell : D^\infty$ and thus, $\tilde{A}(t_1; a, b)$ and $\tilde{B}(t_1; a, b)$ can be obtained simply as the *normal form* of $m'_{t_1}(t_1; a, b)\tilde{a}$ and that of $m'_{t_1}(t_1; a, b)\tilde{b}$ modulo G with respect to a block monomial ordering $<$ such that $\{a, b, t_1\} \ll \{\tilde{a}, \tilde{b}\}$. The details will be given in the next section.

REMARK 4.13 (Multiple Root Case). The set GB shall directly give our formula (Shape Form) for isogeny. However, as the denominators are factors of the discriminant of m_{t_1}, our formulas cannot work when m_{t_1} has multiple roots for values α, β for a, b. But, even in such a case, the ideal $I_\ell : D^\infty$ (which is prime and coincides with I_ℓ^{ec} in our conjecture) itself has a corresponding zero giving a correct isogeny. For finding it, we can use the computed Gröbner basis of $I_\ell : D^\infty$. Thus, we may say the Gröbner basis itself *another formula* that can handle any values α, β for a, b with $D(\alpha, \beta) \neq 0$.

5. Symbolic Computations by Gröbner Bases

Here we report our experiments for computing the symbolic formulas. To make our computation efficient and practical, we apply modular techniques based on Chinese Remainder Theorem and an F_4 type algorithm. All experiments are done using a computer algebra system Risa/Asir. Besides our main goal for obtaining symbolic formulas, the ideals discussed here are very interesting to test our efficient techniques of Gröbner basis computation. Thus, we give details on our Gröbner basis computation.

REMARK 5.1. Our computational goal is to find essential algebraic relations in $I_\ell : D$ based on our conjecture. To do so, there are several approaches and possible efficient combination. For examples, we may use an efficient computation for the minimal polynomial m_{t_1} by [6] and add it to the generators of the ideal. Moreover, we may use *interpolation*

technique as follows; First we evaluate a, b with number of integers for the generating set and consider ideals generated by them. Then, we obtain our formulas without parameter a, b by Gröbner basis computation and recover the true formulas by interpolation. We note that Poteaux and Schost [22] applied *change of basis technique* for computation of m_{t_1} by using the idea in [6], where they obtain m_{t_1} from a triangular set $\{\psi_\ell(x), t + A(x)\}$ for a certain polynomial $A(x)$ constructed by a sum of x-coordinate of multiple points of P with $x = x(P)$. This does not seems to work well on our parametric case, where a, b are indeterminates, because k-th multiplication is complicated rational function, which might makes the total computation worse.

5.1. Main Procedures

First we consider Shape Form formula. Using the properties of I_ℓ given in the previous section, we execute the following steps for making the formula.

REMARK 5.2. We can use an equivalent generating set which is derived as follows: Combining Equations (14) and (5), we can remove the factor F_ℓ^2 from Equation (15).

$$f_{6k+1}x^{6k+1} + f_{6k}x^{6k} + \cdots + f_0 = F_\ell(x)^2 \times (\hat{f}_{4k+1}x^{4k+1} + \cdots \hat{f}_0)\,.$$

From $\hat{f}_{4k+1}, \ldots, \hat{f}_{3k+3}$, we have the polynomials $h_i = t_i - H_i$ shown in Lemma 4.2.

Procedure for Shape Form Formula

STEP 1. COMPUTATION OF GENERATORS OF I_ℓ^0: From the system of algebraic equations (14) and (15), compute all generators f_i of the ideal I_ℓ^0 of $K[a, b, \tilde{a}, \tilde{b}, t_1, \ldots, t_k]$.

STEP 2. COMPUTATION OF GENERATORS OF I_ℓ: Using Lemma 4.2, transform generators f_i to $\tilde{f}_i$ in $K[a, b, \tilde{a}, \tilde{b}, t_1]$. We note that for $2 \le i \le k$, $\tilde{f}_{6k+3-i}$ gives an expression of t_i as a polynomial in $a, b, \tilde{a}, \tilde{b}, t_1$. Then, $G_0 = \{\tilde{f}_{6k+3-i} \mid k + 1 \le i \le 6k + 3\}$ is a generating set of I_ℓ.

STEP 3. COMPUTATION OF GRÖBNER BASIS OF I_ℓ^e: Compute the reduced Gröbner basis GB_1 of the ideal I_ℓ^e generated by G_0 with respect to a block monomial ordering $<$ such that $\{t_1\} \ll \{\tilde{a}, \tilde{b}\}$.

PROPOSITION 5.3. *If the computed Gröbner basis GB_1 is of shape form the same as the formula* (16)*, then I_ℓ^e is shown to be a maximal ideal of $K(a, b)[t_1, \tilde{a}, \tilde{b}]$ and GB_1 gives the correct formula.*

By our conjecture, for each prime ℓ, the computed Gröbner basis GB_1 is of shape form and it shall give our symbolic formula. However, it is very hard to compute GB_1 *directly over* $K(a, b)$, and thus it is better to change the third step as follows:

Modified Step 3.

STEP 3-1. COMPUTATION OF GRÖBNER BASIS OF I_ℓ: As I_ℓ is weighted homogeneous, compute its reduced Gröbner basis G_1 with respect to some *weighted-degree-compatible* monomial ordering.

STEP 3-2. COMPUTATION OF GRÖBNER BASIS OF $I_\ell : D^\infty$: Let $D = 4a^3 + 27b^2$ and u a new variable. Compute the reduced Gröbner basis G_2 of the ideal

$I_\ell : D^\infty$ as the elimination ideal $I' \cap K[a, b, \tilde{a}, \tilde{b}, t_1]$, where I' is generated by G_1 and $uD - 1$, with respect to a *weighted* block monomial ordering $<$ such that $\{a, b, t_1\,\tilde{a}, \tilde{b}\} \ll \{u\}$.

STEP 3-3. COMPUTATION OF GRÖBNER BASIS OF I_ℓ^e: Compute the reduced Gröbner basis GB_1 of the ideal $I_\ell^e = (I_\ell : D^\infty)^e$ generated by G_2 with respect to a weighted monomial ordering $<$ such that $\{t_1\} \ll \{\tilde{a}, \tilde{b}\}$.

We may skip Step 3-1 and compute the Gröbner basis G_2 directly from G_0 and $uD - 1$.

REMARK 5.4. In our case, the selection strategy *SUGAR* on S-pairs works very well by assigning a *virtual* weight -6 to u. (For SUGAR strategy, see [10].) By this assignment, we may tailor certain computational good behavior as a *homogeneous* ideal.

Even if we apply Modified Step 3, it is still hard to compute the Gröbner basis GB_1 over $K(a, b)$ at Step 3-3. Thus, we add a further trick for its computation. Using our observation shown in Section A and Proposition 4.12 we can replace Step 3-3 with the following. This trick can improve the total efficiency very well.

Alternative Procedure to Step 3-3.

STEP I. CHANGE OF ORDERING: We compute the Gröbner basis G_3 with respect to a weighted monomial ordering $<$ such that $\{a, b, t_1\} \ll \{\tilde{a}, \tilde{b}\}$. (Another condition $\{a, b\} \ll \{t_1\} \ll \{\tilde{a}, \tilde{b}\}$ is more suited *in theory* but it might make our Gröbner basis computation inefficient.)

STEP II. COMPUTATION OF $m_{t_1}(t_1; a, b)$: If $G_3 \cap K[a, b, t_1]$ consists of one polynomials which is irreducible in $K[t_1, a, b]$ and monic and of degree $\ell + 1$ with respect to t_1, it is shown to be the minimal polynomial m_{t_1} by Proposition 4.12. (Else our conjecture fails.)

STEP III. COMPUTATION OF POSSIBLE $d_A(a, b)$ AND $d_B(a, b)$: We compute the discriminant of m_{t_1} and, by its square-free factorization, we compute the product $d_{t_1}(a, b)$ of all square factors of the discriminant. By our observation in Section A, we redefine $d_{t_1}(a, b)$ by removing the power of D from $d_{t_1}(a, b)$.

STEP IV. COMPUTATION OF $d_A, d_B, A(t_1), B(t_1)$: First we compute the normal form, say A_0, of $d_{t_1}(a, b)\tilde{a}$ and that, say B_0, of $d_{t_1}(a, b)\tilde{b}$ by using G_3. (Then $\deg_{t_1}(A_0) \le \ell$ and $\deg_{t_1}(B_0) \le \ell$, where $\deg_{t_1}$ denotes the degree in t_1.)

(1) If A_0 or B_0 does not belong to $K[a, b, t_1]$, then our conjecture fails.

(2) Else we compute the GCD, say f_A, of $d_{t_1}(a, b)$ and $A_0(t_1; a, b)$ and that, say f_B, of $d_{t_1}(a,b)$ and $B_0(t_1;a,b)$. Then $\frac{d_{t_1}(a,b)\tilde{a} - A_0(t_1;a,b)}{f_A}$ and $\frac{d_{t_1}(a,b)\tilde{a} - B_0(t_1;a,b)}{f_B}$ give our formula, that is,

$$d_A(a, b) = \frac{d_{t_1}(a, b)}{f_A(a, b)},\ d_B(a, b) = \frac{d_{t_1}(a, b)}{f_B(a, b)},$$

$$A(t_1; a, b) = \frac{A_0(t_1; a, b)}{f_A(a, b)},\ B(t_1; a, b) = \frac{B_0(t_1; a, b)}{f_B(a, b)}.$$

REMARK: By our observation possible common factors f_1, f_2 are small powers of a or those of b.

When the procedure Alternative Procedure to Step 3-3 outputs the polynomials, the correctness can be guaranteed by the following:

PROPOSITION 5.5. *If Alternative Procedure does not fail, output polynomials are correct ones corresponding to Shape Form formula* (8).

Proof. The radical of the generic component $\sqrt{I_\ell^{ec}} : \tilde{D}$ contains $d_A(a,b)\tilde{a} - A(t_1;a,b)$ and $d_B(a,b)\tilde{a} - B(t_1;a,b)$, where $\deg_{t_1}(A) \leq \ell$ and $\deg_{t_1}(B) \leq \ell$. Also, it contains I_ℓ^{ec} and $I_\ell : D^\infty$, and thus it contains $d_{t_1}(a,b)\tilde{a} - A_0(t_1;a,b)$ and $d_{t_1}(a,b)\tilde{a} - B_0(t_1;a,b)$, where $\deg_{t_1}(A_0) \leq \ell$ and $\deg_{t_1}(B_0) \leq \ell$. As d_A divides d_{t_1}, $\sqrt{I_\ell^{ec}} : \tilde{D}$ also contains the following polynomial g:

$$g = d_{t_1}(a,b)\tilde{a} - A_0(t_1;a,b) - \frac{d_{t_1}}{d_A}(d_A(a,b)\tilde{a} - A(t_1;a,b)) = -A_0(t_1;a,b) + \frac{d_{t_1}}{d_A}A(t_1;a,b)\,.$$

Then g belongs to $K[a,b,t_1]$ and it should be divisible by the minimal polynomial $m_{t_1}(t_1;a,b)$. Comparing their degrees with respect to t_1, it follows that $g = 0$. This implies that the output polynomial for $\tilde{a}$ coincides with $d_A(a,b)\tilde{a} - A(t_1;a,b)$. By the same argument, the output polynomial for $\tilde{b}$ also coincides with $d_B(a,b)\tilde{b} - B(t_1;a,b)$. □

REMARK 5.6. The efficiency of Alternative Procedure heavily depends on that of computation of the discriminant, which is the resultant computation of m_{t_1} and its derivative. For the square-free factorization of the discriminant, we can utilize its special structure observed in Section A effectively as follows: After removing powers of $4a^3 + 27b^2$ and small powers of a, b, the remaining is a square of an irreducible polynomial. Thus, we can compute the remaining irreducible factor by a special procedure for polynomial square-root computation. In our experiment, it worked very efficiently. But, even we applied it, computation of Shape Form formulas was still hard due to the growth of their weights.

Using the same technique, we can compute the RUR formula (9) from the Gröbner basis G_3.

Procedure for RUR Formula

STEP A. COMPUTATION OF $m_{t_1}(t_1;a,b)$: The same as Step I and Step II in Alternative Procedure to Step 3-3.

STEP B. COMPUTATION OF $\hat{A}(t_1;a,b)$ AND $\hat{B}(t_1;a,b)$: We compute $\hat{A}(t_1;a,b)$ and $\hat{B}(t_1;a,b)$ as the normal form of $m'_{t_1}(t_1;a,b)\tilde{a}$ and that of $m'_{t_1}(t_1;a,b)\tilde{b}$, respectively, by using G_3. (If the normal form contains $\tilde{a}$ or $\tilde{b}$, our conjecture fails.)

The correctness can be shown in the same manner as the proof of Proposition 5.5. Once we have the Gröbner basis G_3 of $I_\ell : D^\infty$ with respect to a weighted monomial ordering $<$ such that $\{a,b,t_1\} \ll \{\tilde{a},\tilde{b}\}$, the RUR formula can be computed very efficiently. This is because it can be computed very efficiently by the normal form computation and the presentation is very concise.

REMARK 5.7. For getting the RUR formula, we need to handle polynomials of smaller weight only. Therefore, instead of the whole G_3, its subset consisting of such

smaller polynomials are sufficient. (Such a subset can be computed by stopping the Gröbner basis computation *in the middle*.) Also, since the normal form computation heavily depends on the monomial ordering, as a practical strategy, we compute two subsets $G_{3,a}$ and $G_{3,b}$ such that $G_{3,a}$ is a subset of the Gröbner basis with respect to a weighted monomial ordering $<$ such that $\{a, b, t_1\} \ll \{\tilde{a} < \tilde{b}\}$ and $G_{3,b}$ is also a subset of the Gröbner basis with respect to another monomial ordering $<'$ such that $\{a, b, t_1\} \ll' \{\tilde{b} <' \tilde{a}\}$. We use $G_{3,a}$ for computing the normal form of $m'_{t_1}\tilde{a}$ and $G_{3,b}$ for computing that of $m'_{t_1}\tilde{b}$. By our experiment, it is observed that G_3 tends to be huge compared with G_2. So, it is better to stop the Gröbner basis computation in the middle after getting smaller polynomials enough for our normal form computation.

5.2. Practical Use of Subideal

Since the structure of ideal $I_\ell^{ec} : \tilde{D}^\infty$ and that of $I_\ell^e : \tilde{D}^\infty$ are known, we may improve the total efficiency much more by using a *subideal* as follows: In Step 1 and Step 2, we compute a generating set G_0 of the ideal I_ℓ. However, in our experiment, we can generate the correct ideal I_ℓ^e by a smaller subset S_0 of G_0. Using such a smaller generator improves the total efficiency very well. This is because G_0 becomes very huge, as it has $5k + 3$ elements and the last element $\tilde{f}_0$ has its weight $6k+3$. (Even if we use equivalent generators mentioned in Remark 5.2, they become very huge.) For our experiment for $\ell \leq 89$, we choose the first $\lceil \frac{\ell}{3} \rceil + \frac{\ell-1}{2} \approx \frac{5k}{3}$ elements for such a subset S_0, that seems to optimize the total efficiency.

Let I_ℓ^S be the ideal generated by S_0. Suppose that the reduced Gröbner basis GB' of the ideal $(I_\ell^S)^e$ is of shape form the same as in the formula (16). Then, since the number of zeros of $I_\ell^e : \tilde{D}^\infty$ coincides with that of $(I_\ell^S)^e$, it follows that $\sqrt{I_\ell^e} : \tilde{D} = I_\ell^e : \tilde{D}^\infty = (I_\ell^S)^e$ and GB' is the correct basis. In more detail, we have the following which guarantees the correctness of the computation with the subideal. Let S_2 be the Gröbner basis obtained in Modified Step 3 for $I_\ell^S : D^\infty$ and S_3 its another Gröbner basis obtained in Alternative Procedure to Step 3-3. Using the same argument in the proof of Proposition 5.5, the correctness of the computed polynomials are guaranteed as follows:

PROPOSITION 5.8. *Suppose that $S_3 \cap K[a, b, t_1]$ consists of one polynomial $M(t_1; a, b)$ which is irreducible in $K[a, b, t_1]$ and monic and of degree $\ell + 1$ with respect to t_1. Then $M(t_1; a, b)$ coincides with the minimal polynomial $m_{t_1}(t_1; a, b)$. Moreover, the following holds;*

(1) *If there are polynomials $\hat{A}_0(t_1; a, b)$ and $\hat{B}_0(t_1; a, b)$ in t_1, a, b over K such that $\deg_{t_1}(\hat{A}_0) \leq \ell$, $\deg_{t_1}(\hat{B}_0) \leq \ell$ and $I_\ell^S : D^\infty$ contains $m'_{t_1}(t_1; a, b)\tilde{a} - \hat{A}_0(t_1; a, b)$ and $m'_{t_1}(t_1; a, b)\tilde{b} - \hat{B}_0(t_1; a, b)$, then $\hat{A}_0 = \hat{A}$ and $\hat{B}_0 = \hat{B}$. ($\hat{A}_0$ and $\hat{B}_0$ shall be computed as the normal form of $m'_{t_1}\tilde{a}$ and that of $m'_{t_1}\tilde{b}$ by S_3, respectively.)*

(2) *If there are polynomials $A_0(t_1; a, b)$ and $B_0(t_1; a, b)$ in t_1, a, b over K such that $\deg_{t_1}(A_0) \leq \ell$, $\deg_{t_1}(B_0) \leq \ell$ and $I_\ell^S : D^\infty$ contains $d_{t_1}(a, b)\tilde{a} - A_0(t_1; a, b)$ and $d_{t_1}(a, b)\tilde{b} - B_0(t_1; a, b)$, where $d_{t_1}(a, b)$ is the product of all square-free factors of the*

discriminant of m_{t_1} with the power of D eliminated, then

$$\frac{A_0}{d_{t_1}} = \frac{A}{d_A}, \quad \frac{B_0}{d_{t_1}} = \frac{B}{d_B}.$$

(A_0 and B_0 shall be computed as the normal form of $d_{t_1}\tilde{a}$ and that of $d_{t_1}\tilde{b}$ by S_3, respectively.)

As mentioned in Remark 5.7 we need polynomials with smaller weight for the RUR formula. Thus, we can replace S_3 with its subsets $S_{3,a}$ and $S_{3,b}$.

5.3. Formulas for $K = \mathbb{Q}$ by Modular Method

When $K = \mathbb{Q}$, there are techniques called *modular techniques*, by which we can resolve the notorious computational problem called *intermediate coefficient growth*. Here we employ the following technique, where a generating set H of an ideal over $\mathbb{Q}$ and a monomial ordering $<$ are given.

General Procedure of Modular Method based on CRT

STEP 1. MODULAR STEP: We compute reduced Gröbner bases G_p of *projected ideals* over $\mathbb{F}_p$ for several primes p with respect to $<$. Here the projected ideal over $\mathbb{F}_p$ means the ideal $\langle \varphi_p(H) \rangle$ generated by the projected image of $\varphi_p(H)$, where φ_p denotes the natural projection from $\mathbb{Z}_{(p)}[X]$ to $\mathbb{F}_p[X]$. (See Remark 3.12.) It is highly expected that G_p is the projected image of the reduced Gröbner basis G of the ideal generated by H over $\mathbb{Q}$ with respect to $<$.

STEP 2. CRT STEP: From computed Gröbner bases G_p, we compute a candidate G_{can} of the Gröbner basis by *Chinese Remainder Theorem (Algorithm)* and *rational reconstruction*.

STEP 3. VERIFICATION STEP: We check whether G_{can} is the reduced Gröbner basis.

There are two merits for using Modular Method based on CRT; it is suited for parallel computation and it practically detects *unlucky* prime numbers. Here a prime number p is said to be *lucky* if the computed reduced Gröbner basis G_p coincides exactly with the projected image of the reduced Gröbner basis G. We note that there arise a problem on how to provide sufficiently many prime numbers and that on how to discard *unlucky* primes. In many cases, it is hard to predict the luckiness without knowing G, although it is shown that the number of *unlucky* primes is finite. Moreover, it is also hard to give *practical or exact* coefficient bound for Chinese Remainder Theorem *in theory* and we should introduce some *heuristic* bound with *trial-error* for making the total computation very practical. But, for our case, as we know the *shape* of Gröbner basis and ideals are weighted homogeneous, we may resolve those problems rather easily. See [1] for homogeneous ideals and [21] for details on the most recent results.

In more detail, we employ the following general computational flow (see [12]).

CRT Modular Computation for Gröbner Basis

INPUT: a generating set H of an ideal I and a monomial ordering $<$
OUTPUT: the reduced Gröbner basis of I with respect to $<$
Choose $\mathcal{P}$ as a list of random prime numbers;
$\mathcal{GP} = \emptyset$;

loop
  for $p \in \mathcal{P}$ **do**
    compute the reduced Gröbner basis G_p of $\langle \varphi_p(H) \rangle$ w.r.t. $<$;
    $\mathcal{GP} = \mathcal{GP} \cup \{G_p\}$;
  $(\mathcal{HP}_{lucky}, \mathcal{P}_{lucky}) =$ DELETEUNLUCKYPRIMES$(\mathcal{GP}, \mathcal{P})$;
  lift $\mathcal{GP}_{lucky}$ to G_{can} by CRT and rational reconstruction;
  if G_{can} passes VERIFICATION TEST **then**
    return G_{can}
enlarge $\mathcal{P}$ with prime numbers not used so far;

Our Verification Test

As to the correctness of I_ℓ or I_ℓ^S, we can use the result of [1] for rather easier verification by using the property of being weighted homogeneous. In our experiment, we applied more effective verification for efficient computation, where we used a subideal I_ℓ^S generated by a subset S_0 and computed Shape Form formulas and RUR formulas from the computed Gröbner basis S_2 of $I_\ell^S : D^\infty$ by CRT modular computation but without verification $\langle S_2 \rangle = I_\ell^S : D^\infty$, where $\langle S_2 \rangle$ denotes the ideal generated by S_2. (We checked that S_2 is a Gröbner basis of $\langle S_2 \rangle$.) We note that, for each prime number p used in CRT modular computation, we computed the reduced Gröbner basis of the ideal $\langle \varphi_p(S_0) \rangle : \varphi_p(D)^\infty$ in $\mathbb{F}_p[a, b, t_1, \tilde{a}, \tilde{b}]$ as the projected image of $I_\ell^S : D^\infty$, where φ_p denotes the natural projection from $\mathbb{Z}_{(p)}[a, b, t_1, \tilde{a}, \tilde{b}]$ to $\mathbb{F}_p[a, b, t_1, \tilde{a}, \tilde{b}]$. Thus S_2 is still a candidate of the Gröbner basis of $I_\ell^S : D^\infty$.

But, in our case, we can examine not the correctness of S_2 but the the correctness of the computed RUR formula directly by checking the following: (The correctness of the computed Shape Form formula can be checked in the same manner. If S_2 is the verified Gröbner basis of $I_\ell^S : D^\infty$, the property (1) is enough by Proposition 5.8.)

(1) From S_2, we computed another Gröbner basis S_3 (or its subsets $S_{3,a}, S_{3,b}$) by which we obtained a monic and irreducible univariate polynomial M_S in t_1 over $\mathbb{Q}[a, b]$ of degree $\ell + 1$ as a unique element in $S_3 \cap \mathbb{Q}[a, b, t_1]$, and a RUR form $M'_S\tilde{a} - \hat{A}_S$ for $\tilde{a}$ and that $M'_S\tilde{b} - \hat{B}_S$ for $\tilde{b}$ with respect to M_S. ($\hat{A}_S$ and $\hat{B}_S$ are obtained as the normal form of $M'_S\tilde{a}$ and that of $M'_S\tilde{b}$, respectively.)
(2) $I_\ell \subset \langle S_2 \rangle$, that is, all members of G_0 belong to $\langle S_2 \rangle$. We note that it is equivalent to verify that all generators f_i (or $\hat{f}_i$) are reduced to 0 by $S_2 \cup \{h_2, \ldots, h_k\}$, by which we can skip the whole computation of G_0. (For the definition of h_i, see the proof of Lemma 4.2, and for that of $\hat{f}_i$, see Remark 5.2. Also, see Lemma 4.4.)
(3) For any member of S_2, its leading monomial does not belong to $\mathbb{Q}[a, b]$.
(4) $\tilde{D} = D(\tilde{a}, \tilde{b}) = 4\tilde{a}^3 + 27\tilde{b}^2$ does not belong to $\langle S_2 \rangle^e$. Actually this can be checked if M_S does not divide the numerator $4\hat{A}_S^3 + 27M'_S\hat{B}_S^2$ of $D\left(\frac{\hat{A}_S}{M'_S}, \frac{\hat{B}_S}{M'_S}\right)$.

Once the properties (1), (2), (3) and (4) are verified, the correctness of the computed RUR formula can be shown as follows: From (3), we have $\langle S_2 \rangle \cap \mathbb{Q}[a, b] = \{0\}$ by using the property of the Gröbner basis. Moreover, as M_S is irreducible over $\mathbb{Q}(a, b)$, $M'_S\tilde{a} - \hat{A}_S$ is linear in $\tilde{a}$ and $M'_S\tilde{b} - \hat{B}_S$ is also linear in $\tilde{b}$, it follows that $\langle S_2 \rangle^e$ is maximal in

$\mathbb{Q}(a,b)[\tilde{a},\tilde{b},t_1]$. As $I_\ell \subset \langle S_2\rangle$, we also have $I_\ell^e \subset \langle S_2\rangle^e$ and $\sqrt{I_\ell^e} \subset \langle S_2\rangle^e$. Also, as $\tilde{D} = D(\tilde{a},\tilde{b})$ does not belong to $\langle S_2\rangle^e$, we have $\langle S_2\rangle^e : \tilde{D} = \langle S_2\rangle^e$ by the maximality of $\langle S_2\rangle^e$ and thus $\sqrt{I_\ell^e} : \tilde{D} \subset \langle S_2\rangle^e : \tilde{D} = \langle S_2\rangle^e$. Then $\langle S_2\rangle^e$ contains two irreducible polynomials M_S and m_{t_1} in $\mathbb{Q}[t_1,a,b]$. If they differ, their non-zero resultant belongs to $\mathbb{Q}[a,b]$, which implies $\langle S_2\rangle \cap \mathbb{Q}[a,b] \neq \{0\}$ and a contradiction. Thus, $M_S = m_{t_1}$. In a similar manner, we can show $\hat{A} = \hat{A}_S$ and $\hat{B} = \hat{B}_S$. We remark that $(M'_S)^3\tilde{D} = 4(M'_S\tilde{a})^3 + 27M'_S(M'_S\tilde{b})^2 \equiv 4\hat{A}_S^3 + 27M'_S\hat{B}_S^2$ modulo $\langle S_2\rangle^e$ and M'_S does not belong to $\langle S_2\rangle^e$. Thus, if $4\hat{A}_S^3 + 27M'_S\hat{B}_S^2$ does not belong to $\langle S_2\rangle^e$ then $\tilde{D}$ does not belong to $\langle S_2\rangle^e$. Also, $\langle S_2\rangle^e \cap \mathbb{Q}(a,b)[t_1]$ is a principal ideal generated by M_S and its membership can be decided by its divisibility by M_S.

We checked the properties (1), (2), (3) and (4) for all computed Gröbner bases up to $\ell = 83$. Thus, those formulas are verified to be correct.

Experimental Data

Table 1 shows some timing data for computation of the Gröbner S_2 basis of $I_\ell^S : D^\infty$ with respect to a weighted block monomial ordering $<$ such that $\{a,b,t_1\} \ll \{\tilde{a},\tilde{b}\}$ for several primes ℓ by using our modular techniques and subideals *without verification* $\langle S_2\rangle = I_\ell^S : D^\infty$, where our subideal I_ℓ^S was generated by a subset S_0 with $\lceil \frac{\ell}{3} \rceil + \frac{\ell-1}{2}$ elements. Also we apply the *virtual weight* mentioned in Remark 5.4. The timings (in seconds) for computing S_2 were measured on a PC with 4 Xeon E5-4617 CPUs, where 20 parallel processes were used.

ℓ	41	43	47	53	59	73	79
S_1	421.7	621.3	1789	4777	14970	201500	353900

TABLE 1. Timings of Computation of S_1

The practical behavior on our computation in Table 1 suggests that the cost can be roughly estimated as $O(\ell^{10})$ by seeing the ratios. We have also computed the reduced Gröbner basis without complete verification and the RUR formula for $\ell = 87$ which was adopted for SEA algorithm in Section 6.1.

After getting the Gröbner basis S_2 of $I_\ell^S : D^\infty$, other Gröbner bases $G_{3,a}$ and $G_{3,b}$ (up to necessary degrees) were computed, by which the RUR formulas were computed directly by normal form computation. The timings (in seconds) in Table 2 for computing $S_{3,a}$, $S_{3,b}$ were measured on the same PC but with 10 parallel processes.

ℓ	41	43	47	53	59	73	79
$S_{3,a}$	7.986	11.34	17.01	39.17	80.81	420.6	705.0
$S_{3,b}$	11.91	20.29	31.75	79.54	189.9	977.4	1463

TABLE 2. Timings of $S_{3,a}$ and $S_{3,b}$

6. Correctness on Computed Formulas and Application

The computed formulas (and Gröbner bases) can be used for further numerical computations related to elliptic curves. By these applications, we can examine the correctness and also the applicability of our computed formulas.

6.1. Direct Application to SEA Algorithm of Point Counting

To ensure the correctness and applicability of our computed formulas, we adopted them to so called SEA (Schoof-Elkies-Atkin) algorithm for counting the number of rational points of an elliptic curve over a finite field. Our adoption is done by replacing (canonical) modular polynomials with minimal polynomials of t_1 for each odd prime and computing the Elkies polynomials (factors) by using our RUR formulas. Once we evaluate a and b in our RUR formula, it can be shown that, except for cases of multiple roots, the factorization pattern of the minimal polynomial m_{t_1} satisfies the properties of the modular polynomial Φ_ℓ given in Proposition 12.20 and Theorem 12.22 in [30]. Here we summarize how the isogeny computation by our formulas can be used for SEA algorithm:

Let p be a prime, $E(a, b)$ an elliptic curve defined over a finite field $\mathbb{F}_p$ and ℓ an odd prime much smaller than p. (Thus a, b belong to $\mathbb{F}_p$.) In SEA algorithm we consider a possible isogeny of degree ℓ. The number of rational points of $E(a, b)$ over $\mathbb{F}_p$ is expressed as $p + 1 - T$, where T is so-called the *trace* of the Frobenius map. By our formulas, we can deduce the following, where we assume that $m_{t_1}(= m_{t_1}(t_1; a, b))$ has no multiple root.

- If m_{t_1} has no rational root over $\mathbb{F}_p$, then ℓ is an *Atkin* prime, and the factorization pattern of m_{t_1} over $\mathbb{F}_p$ gives a very useful information of possible values of the trace T modulo ℓ of the Frobenius map.
- If m_{t_1} has a rational root τ over $\mathbb{F}_p$, we get the values $\tilde{\alpha}$ and $\tilde{\beta}$ by the RUR formula and the Elkies polynomial F_ℓ. Then, by using F_ℓ, we compute the eigenvalue of the Frobenius map acting on $E[\ell]$ and the value of its trace T modulo ℓ.

We implemented our adoption to the SEA implementation in [13], where several techniques for improving the efficiency including *isogeny double* are used. As we have computed the RUR formulas only for smaller primes, we compared our adoption and the original SEA implementation for 160-bit size finite fields $\mathbb{F}_p$ which can be used for actual elliptic curve cryptosystems. As a result, our adoption computed the correct outputs for all sampled elliptic curves, which *assures the correctness* of our RUR formulas. As to the total efficiency, our *simple* adoption is *comparable* to the original SEA implementation. This is because the order of the complexity does not change by our adoption. Table 3 shows some timing data for required seconds for counting the number of rational points of elliptic curves $E(a, b)$ over $\mathbb{F}_p$, where $p = 2^{160} - 75$, a 160-bit prime, and $a = 1$ and $1 \leq b \leq 300$. Timings (in seconds) are measured on a PC with Xeon E5-1650v2 of 3.5 GHz.

Implementation	Average	Max	Min
SEA	1.32	3.40	0.78
SEA with RUR Formula	1.38	3.34	0.81

TABLE 3. Timings of SEA and SEA with RUR Formula

6.2. Computation of Modular Polynomial

Once we have a Gröbner basis, by using *elimination ideals*, we can compute essential algebraic relations among specified variables. As an example, the modular polynomial of order ℓ can be obtained by this technique. For an elliptic curve $E(a, b)$, its j-invariant, denoted by $j(a, b)$, is defined as

$$j(a,b) = \frac{1728 \times 4a^3}{4a^3 + 27b^2} = \frac{6912a^3}{D(a,b)}$$

Introducing two variables j, $\tilde{j}$, we consider the ideal $\mathcal{J}_\ell$ generated by $\hat{I}_\ell^e$, $D(a,b)j - 6912a^3$ and $D(\tilde{a},\tilde{b})\tilde{j} - 6912\tilde{a}^3$ in $K(a,b)[\tilde{a},\tilde{b},t_1,u,j,\tilde{j}]$. Then there is one to one correspondence between the varieties (sets of zeros) $V_{\overline{K(a,b)}}(\hat{I}_\ell^e)$ and $V_{\overline{K(a,b)}}(\mathcal{J}_\ell)$ as follows:

$$V_{\overline{K(a,b)}}(\hat{I}_\ell^e) \ni (\tilde{\alpha},\tilde{\beta},\tau,\upsilon) \leftrightarrow (\tilde{\alpha},\tilde{\beta},\tau,\upsilon,\iota,\tilde{\iota}) \in V_{\overline{K(a,b)}}(\mathcal{J}_\ell)\,.$$

Then $\mathcal{J}_\ell$ is 0-dimensional ideal with $\ell+1$ distinct zeros, and $E(a,b)$ and $E(\tilde{\alpha},\tilde{\beta})$ are isogeny elliptic curves. Thus, their j-invariants $\iota = j(E(a,b))$ and $\tilde{\iota} = j(E(\tilde{\alpha},\tilde{\beta}))$ should satisfies the modular polynomial Φ_ℓ of order ℓ for $K = \mathbb{Q}$ and its modular image $\varphi_p(\Phi_\ell)$ for $K = \mathbb{F}_p$. By Hilbert's Nullstellensatz, it should belong to the radical of $\mathcal{J}_\ell$. This gives the following lemma.

LEMMA 6.1. *Some power of $\Phi_\ell(j,\tilde{j})$ or its modular image $\varphi_p(\Phi_\ell)$ belongs to $\mathcal{J}_\ell$ and so belongs to its elimination ideal $\mathcal{J}_\ell \cap K[j,\tilde{j}]$. If our conjecture holds, it belongs to $\mathcal{J}_\ell$ and so belongs to its elimination ideal $\mathcal{J}_\ell \cap K[j,\tilde{j}]$.*

From our conjecture and experience, the ideal $\mathcal{I}_\ell$ generated by I_ℓ, $D(a,b)u-1$, $D(a,b)j - 6912a^3$ and $D(\tilde{a},\tilde{b})\tilde{j} - 6912\tilde{a}^3$ in $K[a,b,\tilde{a},\tilde{b},t_1,u,j,\tilde{j}]$ contains a polynomial in j and $\tilde{j}$ over K. It can be shown that the polynomial coincides with $\Phi_\ell(j,\tilde{j})$ or its projected image. Thus, using a block monomial ordering $\{a,b,\tilde{b},\tilde{a},t_1,u\} \gg \{j,\tilde{j}\}$, we find $\Phi_\ell(j,\tilde{j})$ in its Gröbner basis. It is not an efficient way to use our formulas (Gröbner bases) for computing modular polynomials over $\mathbb{Q}$, since efficient numerical methods on floating arithmetics are already given. But, our method is based on *exact computation and purely algebraic*, by which their modular images can be computed directly over $\mathbb{F}_p$.

7. Concluding Remarks

In this paper we considered possible symbolic formulas of the isogeny ϕ of degree ℓ between elliptic curves $E(a,b)$ and $E(\tilde{a},\tilde{b})$ defined by $y^2 = x^3 + ax + b$ and $y^2 = x^3 + \tilde{a}x + \tilde{b}$, respectively. Our target is to express $\tilde{a}$, $\tilde{b}$ and all coefficients of the Elkies polynomial F_ℓ as certain functions in a and b. Considering $E(a,b)$ over $K(a,b)$, we derived the symbolic formulas. Then, by using algebraic relations derived from Vélu's formula, we proved that those can be obtained as elements in an ideal generated by all algebraic constraints derived from Vélu's formula. To obtain those formulas explicitly, we adopted Gröbner basis computation as a purely algebraic tool. As results, we succeeded in getting our symbolic formulas for small primes ℓ. In more detail, we obtained the following:

- By purely algebraic argument, we succeed in expressing essential algebraic relations as a *shape form* in variables $t_1, \tilde{a}, \tilde{b}, t_2, \ldots, t_k$ over $\mathbb{Q}(a, b)$, where $k = \frac{\ell-1}{2}$ and $F_\ell(x) = x^k + t_1 x^{k-1} + \cdots + t_k$. The coefficient t_1 is in *generic position* and has its minimal polynomial over $\mathbb{Q}[a, b]$ of degree $\ell + 1$. Other variables $\tilde{a}, \tilde{b}, t_2, \ldots, t_k$ are expressed as polynomials in t_1 over $\mathbb{Q}(a, b)$. Also, as a concise formula, other variables $\tilde{a}, \tilde{b}, t_2, \ldots, t_k$ are expressed as RUR (rational functions) in t_1 over $\mathbb{Q}(a, b)$, whose denominator is the derivative of the minimal polynomial of t_1.
- Our precise analysis on the ideal generated by algebraic constraints derived from Vélu's formula show that each zero of the ideal with $4\tilde{a}^3 + 27\tilde{b}^2 \neq 0$ gives exactly a correct isogeny.
- Those formulas can be computed on real computer by using *efficient modular techniques* for Gröbner bases computation. In particular, the RUR formulas were computed successfully and verified up to $\ell = 83$. Also, their computation over finite fields can be also efficiently done by using the property of being *weighted* homogeneous. The computed formula can be adopted very easily to SEA algorithm of counting rational points of elliptic curves over finite fields. Our implementation can compute the correct answer which guarantees the correctness of our formula.

Computation of our symbolic formulas heavily depends on that of Gröbner basis for the ideal related to the algebraic constraints derived from Vélu's formula. Thus, to compute our formulas for primes ℓ as larger as possible is a good test suite for making efficient methods for Gröbner bases computation, and we applied the most recent modular techniques. Also, we may apply *interpolation* technique for it. For our further improvements, we may combine other methods and ideas, such as those in [6] and [22]. Such improvements are expected to help our further task for handling larger primes ℓ.

Finally we remark that, from the computed formulas, we found some interesting numerical properties which are given in Section A. It would be very nice if such numerical properties might introduce new insights on theory of elliptic curves.

Acknowledgment. The authors are thankful to FUJITSU LABORATORIES LTD. for allowing them to adopt the computed formulas to the SEA implementation that FUJITSU LABORATORIES LTD. owns. They are grateful to the referee for giving various helpful suggestions.

References

[1] E. E. Arnold, Modular algorithms for computing Gröbner bases, Journal of Symbolic Computation **35**, 403–419, 2003.

[2] M. F. Atiyah and I. G. MacDonald, Introduction to Commutative Algebra, Addison-Wesley Series in Mathematics, WESTVIEW PRESS Oxford, 1969.

[3] T. Becker and V. Weispfenning, Gröbner Basis, Graduate Texts in Mathematics **141**, Springer-Verlag New York, 1993.

[4] I. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography, London Mathematical Society Lecture Note Series **265**, Cambridge University Press, 1999.

[5] A. Bostan, F. Morain, B. Salvy and É. Schost, Fast algorithms for computing isogenies between elliptic curves, Mathematics of Computation **77**, 1755–1778, 2008.

[6] L. S. Charlap, R. Coley and D. P. Robbins, Enumeration of rational points on elliptic curves over finite fields, preprint, 1991.
[7] A. C. Cojocaru, D. Grant and N. Jones, One-parameter families of elliptic curves over Q with maximal Galois representations, Proceedings of the London Mathematical Society **103**, 654–675, 2011.
[8] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms 4th Edition, Undergraduate Texts in Mathematics, Springer-Verlag New York, 2015.
[9] L. Dewaghe, Isogénie entre courbes elliptiques, Utilitas Mathematica **55**, 123–128, 1999.
[10] A. Giovini, T. Mora, G. Miesi, L. Robbiano, and C. Traverso, "One Sugar cube, please" or selection strategies in the Buchberger algorithm, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, 49–54, 1991.
[11] G.-M. Greuel and G. Pfister, A Singular Introduction to Commutative Algebra, Springer-Verlag New York, 2002.
[12] N. Idrees, G. Pfister and S. Steidel, Parallelization of modular algorithms, Journal of Symbolic Computation **46**, 672–684, 2011.
[13] T. Izu, J. Kogure, M. Noro, and K. Yokoyama, Efficient implementation of Schoof's algorithm, Advances in Cryptology - ASIACRYPT '98, Lecture Note in Computer Science **1514**, 66–79, 1998.
[14] C. U. Jensen, A. Ledet and N. Yui, Generic Polynomials, Mathematical Science Research Institute Publication **45**, Cambridge University Press, 2002.
[15] N. Jones, Almost all elliptic curves are Serre curves, Transactions of the American Mathematical Society **362**, 1547–1570, 2010.
[16] D. Kohel, Endomorphism rings of elliptic curves over finite fields, PhD thesis, University of California at Berkeley, 1996.
[17] M. Kreuzer and L. Robbiano, Computational Commutative Algebra 2, Springer-Verlag New York, 2005.
[18] R. Lercier and T. Sirvent, On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field, Journal de théorie des nombres de Bordeaux **20**, 783–797, 2008.
[19] F. Morain, Calcul du nombre de points sure une courbe elliptique dan un corps fini:aspects algorithmiques, Journal de théorie des nombres de Bordeaux **7**, 255–282, 1995.
[20] M. Nagata, Local Rings, Interscience Tracts in Pure and Applied Mathematics **13**, John Wiley & Sons Inc New York, 1962.
[21] M. Noro and K. Yokoyama, Usage of modular techniques for efficient computation of ideal operations, Mathematics in Computer Science **12**, 1–32, 2018.
[22] A. Poteaux and É. Schost, Modular composition modulo triangular sets and applications, Computational Complexity **22**, 463–516, 2013.
[23] F. Rouillier, Solving zero-dimensional systems through the rational univariate representation, Appl. Algebra Eng. Commm. Comput. **5**, 433–461, 1999.
[24] R. Schoof, Counting points on elliptic curves over finite fields, Journal de théorie des nombres de Bordeaux **7**, 219–254, 1995.
[25] J.-P. Serre, Propriétés galoisiennes des points d'order fini des courbes elliptiques, Inventiones Mathematics **15**, 259–311, 1972.
[26] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics **151**, Springer-Verlag New York, 1994.
[27] J. H. Silverman, The arithmetic of elliptic curves 2nd Edition, Graduate Texts in Mathematics **106**, Springer-Verlag New York, 2009.
[28] W. V. Vasconcelos, Computational Methods in Commutative Algebra and Algebraic Geometry, Algorithms and Computation in Mathematics **2**, Springer-Verlag New York, 1998.
[29] J. Vélu, Isogénies entre courbes elliptiques, Comptes Rendus l'Acad. Sci. Paris Série A **273**, 238–241, 1971.
[30] L. C. Washington, Elliptic Curves 2nd Edition, Discrete Mathematics and Its Application **50**, CRC Press New York, 2008.

A. Examples and Observation

Here we give symbolic formulas for small primes computed by our methods and we show several interesting properties found by those examples. Actually, we have computed Shape Form formulas (modified) up to $\ell = 37$ and RUR formulas up to $\ell = 89$.

EXAMPLE A.1. For $\ell = 5$, we have

$$m_{t_1} = t_1^6 + 20at_1^4 - 160bt_1^3 - 80a^2t_1^2 + 128bat_1 - 80b^2, \quad \operatorname{disc}(m_{t_1}) = -2^{26}3^65^5b^2(4a^3 + 27b^2)^4,$$

$$\begin{aligned}\tilde{a} &= \frac{t_1^5 + 20at_1^3 - 200bt_1^2 - 80a^2t_1 + 50ba}{2b} \\ &= \frac{630at_1^5 - 9360bt_1^4 - 8240a^2t_1^3 + 24480bat_1^2 + (1120a^3 - 28800b^2)t_1 - 3200ba^2}{m'_{t_1}},\end{aligned}$$

$$\begin{aligned}\tilde{b} &= 35t_1^3 + 112at_1 - 195b \\ &= \frac{15630bt_1^5 + 34720a^2t_1^4 - 208240bat_1^3 + (-76160a^3 + 110400b^2)t_1^2 + 138720ba^2t_1 - 83200b^2a}{m'_{t_1}},\end{aligned}$$

$$t_2 = \frac{30t_1^2 + 19a + \tilde{a}}{60} = \frac{t_1^5 + 20at_1^3 - 140bt_1^2 - 80a^2t_1 + 88ba}{2^33^15^1b}.$$

For $\ell = 7$, we have

$$\begin{aligned}m_{t_1} &= t_1^8 + 84at_1^6 - 1512bt_1^5 - 1890a^2t_1^4 + 9072bat_1^3 + (644a^3 - 21168b^2)t_1^2 - 5832ba^2t_1 \\ &\quad -567a^4,\end{aligned}$$

$$\operatorname{disc}(m_{t_1}) = 2^{48}3^{16}7^7a^4(11236a^3 + 84035b^2)^2(4a^3 + 27b^2)^6,$$

$$\begin{aligned}\tilde{a} &= \frac{1}{2^13^1a(11236a^3 + 84035b^2)} \\ &\quad \times(-12005bt_1^7 + 3710a^2t_1^6 - 999845bat_1^5 + (308990a^3 + 18151560b^2)t_1^4 \\ &\quad +17794105ba^2t_1^3 + (-8388310a^4 - 130518360b^2a)t_1^2 + (13215825ba^3 + 254121840b^3)t_1 \\ &\quad +358386a^5 + 24706290b^2a^2) \\ &= \frac{1}{m'_{t_1}} \times (2408at_1^7 - 75600bt_1^6 - 150696a^2t_1^5 + 1126440bat_1^4 + (183960a^3 - 3810240b^2)t_1^3 \\ &\quad -2013984ba^2t_1^2 + (-317912a^4 + 864864b^2a)t_1 + 285768ba^3),\end{aligned}$$

$$\begin{aligned}\tilde{b} &= \frac{1}{2^13^1a^2(11236a^3 + 84035b^2)} \times ((-16430a^3 - 84035b^2)t_1^7 - 12005ba^2t_1^6 \\ &\quad +(-1376410a^4 - 7058940b^2a)t_1^5 + (23842315ba^3 + 127060920b^3)t_1^4 \\ &\quad +(33215630a^5 + 190843485b^2a^2)t_1^3 + (-131258855ba^4 - 762365520b^3a)t_1^2 \\ &\quad +(379162a^6 + 307861610b^2a^3 + 1778852880b^4)t_1 + 32653257ba^5 + 172944030b^3a^2) \\ &= \frac{1}{m'_{t_1}} \times (117656bt_1^7 + 549024a^2t_1^6 - 7411320bat_1^5 + (-6891360a^3 + 9064440b^2)t_1^4 \\ &\quad +37051560ba^2t_1^3 + (3259872a^4 - 78028272b^2a)t_1^2 + (-21331016ba^3 + 6054048b^3)t_1\end{aligned}$$

$$-1820448a^5 + 2000376b^2a^2),$$

$$t_2 = \frac{30t_1^2 + 29a + \tilde{a}}{60}$$
$$= \frac{1}{2^3 3^2 a(11236a^3 + 84035b^2)} \times (-2401bt_1^7 + 742a^2t_1^6 - 199969bat_1^5$$
$$+(61798a^3 + 3630312b^2)t_1^4 + 3558821ba^2t_1^3 + (-1273166a^4 - 23078412b^2a)t_1^2$$
$$+(2643165ba^3 + 50824368b^3)t_1 + 462690a^5 + 7865676b^2a^2),$$

$$t_3 = \frac{70t_1^3 + (119a + 7\tilde{a})t_1 + 166b + 2\tilde{b}}{420}$$
$$= \frac{1}{2^3 3^2 7^1 a^2(11236a^3 + 84035b^2)} \times ((-1378a^3 - 33614b^2)t_1^7 + 7203ba^2t_1^6$$
$$+(-117978a^4 - 2823576b^2a)t_1^5 + (2683443ba^3 + 50824368b^3)t_1^4$$
$$+(2486442a^5 + 53143734b^2a^2)t_1^3 + (-23177679ba^4 - 304946208b^3a)t_1^2$$
$$+(2257906a^6 + 71715224b^2a^3 + 711541152b^4)t_1 + 5769945ba^5 + 85917384b^3a^2).$$

Observation from Computed Examples

For smaller odd primes ℓ greater than 3 and up to 89, the minimal polynomial m_{t_1} is defined over $\mathbb{Z}[a, b]$. Also, polynomials $A(t_1; a, b)$, $B(t_1; a, b)$, $\hat{A}(t_1; a, b)$, $\hat{B}(t_1; A, B)$ are polynomials over $\mathbb{Z}[a, b]$. This might indicate that $t_1, \tilde{a}, \tilde{b}$ are integral over $\mathbb{Z}[a, b]$. Here we give the sizes of formulas and comparison with that of the modular polynomial Φ_ℓ of order ℓ. Here we use the bit-sizes of their data in Risa/Asir system and, in the table, CAN means the size of a variant (called a canonical modular polynomial) of the modular polynomial proposed by [19] and RUR means the total size of the triple $[m_{t_1}, m'_{t_1}\tilde{a} - \hat{A}, m'_{t_1}\tilde{b} - \hat{B}]$ of polynomials over $\mathbb{Z}$.

ℓ	7	11	13	17	19	23	29	31	37	41	43
m_{t_1}	548	1100	1358	2242	2688	3924	6038	6888	9802	12222	13536
Φ_ℓ	2950	8754	13102	27082	36398	62798	122810	148686	251950	344230	396722
CAN	342	1438	532	1802	1594	6714	5210	3982	3094	11230	7922
RUR	2902	5698	7366	11682	14226	20354	31614	36070	51534	63974	70814

47	53	59	61	67	71	73	79	83	89
16460	21370	27312	29262	36420	41868	44458	53876	60772	72038
521042	752178	1045786	1157530	1547114	1853206	2018422	2580386	3011078	3743498
40638	20926	76190	8122	21966	129298	11930	32710	204082	80494
85858	111514	142042	152802	189658	217450	231654	279754	315050	373154

TABLE 4. Size of Formulas

Table 4 shows that the minimal polynomial m_{t_1} is very concise and *comparable to or sometime much smaller than* the canonical modular polynomial, and moreover, the RUR formula is also concise. On the other hand, the size of the Shape Form formula is very huge due to the growth of the denominators d_A and d_B which will be discussed just below.

Table 5 shows its binary size in Risa/Asir system, where SHAPE means the size of the triple $[m_{t_1}, d_A\tilde{a} - A, d_B\tilde{b} - B]$.

ℓ	7	11	13	17	19	23	29	31	37
SHAPE	2444	12186	21132	66054	104828	259298	767042	1077092	2588626

TABLE 5. Size of Shape Form

As to the discriminant of m_{t_1}, for smaller primes ℓ, it has a special form

$$\pm 2^{\alpha} 3^{\beta} \ell^{\ell} a^{\gamma} b^{\delta} (4a^3 + 27b^2)^{\ell-1} g_{\ell}(a, b)^2 ,$$

where $\alpha, \beta, \gamma, \delta$ are non-negative integers and $g_{\ell}(a, b)$ is an irreducible polynomial in a, b over $\mathbb{Z}$ or 1 for $\ell = 3$ and 5. Table 6 shows the values of $\alpha, \beta, \gamma, \delta$ for smaller primes. From Table 6 it is shown that m_{t_1} is also square-free over a finite field whose characteristic is neither 2,3 nor ℓ. Moreover, it is interesting that a appears as a factor if and only if $\ell \not\equiv 2 \pmod 3$ and b appears as a factor if and only if $\ell \not\equiv 3 \pmod 4$. This might suggest some connection to the supersingularity of curves over the finite field $\mathbb{F}_{\ell}$ of order ℓ.

ℓ	α	β	γ	δ	weight of g_{ℓ}	ℓ	α	β	γ	δ	weight of g_{ℓ}
11	112	36	0	0	36	23	496	180	0	0	210
13	186	70	4	2	48	29	890	282	0	2	348
17	276	102	0	2	102	31	896	358	4	0	402
19	344	160	4	0	132	37	1354	574	4	2	588

TABLE 6. Indices of Factors of $\mathrm{disc}(m_{t_1})$

Also, as to the denominators d_A and d_B, they have the following form for smaller primes ℓ:

$$2^{\alpha'} 3^{\beta'} a^{\gamma'} b^{\delta'} g_{\ell}(a, b) .$$

Thus, the weight of d_A is almost the same as that of g_{ℓ} which seems to grow in ℓ^2-order and much larger than that of m'_{t_1}. Actually, it is expressed as $\frac{(\ell-2)(\ell-3)}{2} - (\gamma + \frac{3}{2}\delta)$ and $\gamma + \frac{3}{2}\delta$ is very small. This fact suggests strong superiority of RUR formulas to Shape Form formulas, since the weight of the denominator m'_{t_1} of RUR is ℓ. Table 7 shows the values of $\alpha', \beta', \gamma', \delta'$.

d_A:

ℓ	α'	β'	γ'	δ'
11	4	2	0	0
13	11	6	1	1
17	13	4	0	1
19	12	7	1	0
23	14	6	0	0
29	24	8	0	1

d_B:

ℓ	α'	β'	γ'	δ
11	4	1	0	0
13	11	7	2	0
17	10	5	0	0
19	12	8	2	0
23	15	7	0	0
29	24	9	0	0

TABLE 7. Indices of Factors of d_A, d_B

As to the factor $g_\ell(a, b)$, since it gives an algebraic constraint between a, b such that m_{t_1} is not square free, it shall give a constraint on the j-invariant of such curves. By using the algebraic relation $(4a^3 + 27b^2)j = 1728 \times 4a^3$ among j and a, b, we can derive an algebraic constraint on j as a polynomial, say $h_\ell(j)$, in j over $\mathbb{Z}$ via Gröbner basis computation, where we excluded a power of a. (See Section 6 for the technique.) For examples, $h_7(j) = 128j - 2268945$ and

$$\begin{aligned} h_{11}(j) = {} & 48828125j^6 - 410405299436664j^5 - 848915250745862831760j^4 \\ & + 285191005864931875240588 80j^3 - 700712570088775459005215040 00j^2 \\ & + 210942137272133340406677906432 0j + 303206106323541624387388060361564 16 . \end{aligned}$$

Table 8 shows the computed degrees of h_ℓ for smaller primes ℓ, which suggest that the weight of g_ℓ coincides with the degree of h_ℓ times 6.

ℓ	7	11	13	17	19	23	29	31	37	41	43	47
degree	1	6	8	17	22	35	58	67	98	123	136	165

TABLE 8. Degree of h_ℓ

Masayuki NORO
Department of Mathematics,
Rikkyo University
3–34–1 Nishi-Ikebukuro, Toshima-ku, Tokyo,
171–8501, Japan
e-mail: noro@rikkyo.ac.jp

Masaya YASUDA
Department of Mathematics,
Rikkyo University
3–34–1 Nishi-Ikebukuro, Toshima-ku, Tokyo,
171–8501, Japan
e-mail: myasuda@rikkyo.ac.jp

Kazuhiro YOKOYAMA
Department of Mathematics,
Rikkyo University
3–34–1 Nishi-Ikebukuro, Toshima-ku, Tokyo,
171–8501, Japan
e-mail: kazuhiro@rikkyo.ac.jp