Two researches on elliptic curves: the rank problem in cyclotomic towers of function fields and an application to integer factorization using the CM method

（楕円曲線に関する二つの研究: 関数体の円分拡大列における
ランク問題と素因数分解への CM 法を用いた応用）

Yusuke AIKAWA

Department of Mathematics
Hokkaido University

March, 2019.

Introduction

This thesis consists of two independent works, which are common in that they deal with elliptic curves. Throughout the thesis, we use terms "the first work" and "the second work" to represent these works. The first work, which is based on [1], is a research on ranks of elliptic curves over the function field $\mathbb{C}(t)$. The second work is an application of elliptic curves to integer factorizations. This is a joint-work with Koji Nuida and Masaaki Shirase [2] [1] .

Background to the First Work

We give an introduction to the first work. Solving systems of algebraic equations over a field is one of the most important problems in number theory. Such problems are called the Diophantine problem. Although this is a simple question, in most cases it is extremely difficult to solve. However, in the process of investigating this problem, we have been making mathematics progress. In fact, such problems, e.g., Fermat's Last Theorem, often lead us to develop more sophisticated theories, tools and methods. In such history, elliptic curves, which are defined by a single cubic equation, have been playing a pivotal role. Thus the arithmetic theory of elliptic curves is a central topic in number theory. The purpose of this thesis is studying the arithmetic properties of elliptic curves over the function field $\mathbb{C}(t)$.

To be more precise, let k be a field and E an elliptic curve over k. As is well known, the set of rational points $E(k)$ i.e., the set of solutions in k of the cubic equation defining E, carries a structure of abelian group, which

[1] This paper entitled "Elliptic Curve Method using Complex Multiplication Method", by the same authors, is published in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Copyright(C) 2019 IEICE.

is called the Mordell-Weil group. The Mordell-Weil theorem states that this group is finitely generated in the arithmetic situation, namely k is a number field or the function field of an algebraic curve over a finite field or the field of complex numbers. The rank of $E(k)$ as a finitely generated abelian group is called the Mordell-Weil rank of E. The Mordell-Weil rank of elliptic curves have been attracting our interest, and there are many variational problems on this quantity. For example, the most famous problem is the Birch and Swinnerton-Dyer conjecture on elliptic curves over $\mathbb{Q}$, which predicts that the Moredell-Weil rank agrees with the pole order of the L-function of elliptic curve. However, there is a dearth of information.

In the first work, as mentioned above, we study the Mordell-Weil group $E(k)$ when k is a function field of an algebraic curve over $\mathbb{C}$. Since this is a finitely generated group if E/k satisfies certain condition [24], we shall discuss a function field analogue of Mazur's conjecture [17], namely the rank growth of $E(k_n)$ for k_n/k a cyclotomic tower.

Background to the Second Work

The second work focuses on algorithmic aspects of elliptic curves. In the second work, we propose algorithms to integer factorization using elliptic curves.

Why integer factoring algorithm? The computational hardness of integer factorization secures a large fraction of the currently known public key cryptosystems, such as well known RSA cryptosystem. Accordingly, study of integer factorization algorithms are not only an interesting mathematical problem but also valuable in order to closely evaluate the actual security level of those cryptosystems in real environments. Now we note that, there are integer factorization algorithms (such as Pollard's $p-1$ method) that work efficiently when the input composite integer satisfies a certain condition depending on each algorithm. By virtue of such special-purpose integer factorization algorithms, the strength of composite integers as secret keys are not uniform even if their bit lengths are equal. From the point of view, it is meaningful to determine the class of easy-to-factorize integers in order to avoid a use of weak keys in practically implemented cryptosystems.

Along this direction of research, recently Shirase [25] proposed a special-

purpose efficient integer factorization algorithm, which is a modification of celebrated Elliptic Curve Method (invented by Lenstra Jr. [16], ECM for short) combined with Complex Multiplication method (CM method for short), the latter being an algorithm to generate an elliptic curve having a certain special property. This algorithm works in polynomial time for a composite having a prime factor of special form which is related to the complex multiplication theory. However, the range of application of the algorithm is strongly limited. In the second work, we give a generalization of this algorithm and extend the range of application.

Our Contributions

The main result of the first work is to present new examples of elliptic curves E over $\mathbb{C}(t)$ having the bounded ranks for the cyclotomic extensions $\mathbb{C}(t^{\frac{1}{n}})/\mathbb{C}(t)$, which are positive examples for a function field analogue of Mazur's conjecture. The main theorem is stated in Theorem 3.2.6. Several positive examples have already been constructed by Stiller [30] and Fastenberg [12], [13]. However, our examples are essentially different from their examples. In fact, their argument is not enough to compute the rank of our examples (for details, see § 2.3). The most salient feature of our work is applying the theory of the monodromy of Gaussian hypergeometric functions to compute the rank of such elliptic curves. This method is developed in § 3.3.

On the other hand, in the second work, we propose a new efficient algorithm to factoring integers, which is an improvement of the previous Shirase's work [25]. Shirase's algorithm factors composite numbers having a prime factor p of special form; $p = 1 + Dv^2$ ($v \in \mathbb{Z}$). However, Shirase's algorithm is effective only for restricted cases. More precisely, the condition for the prime $p = 1 + Dv^2$ in Shirase's algorithm is closely related to a special kind of polynomial called a class polynomial of a discriminant $-D$, and Shirase's algorithm is designed in an ad hoc manner specific to the case where the corresponding class polynomial has degree at most two. In the second work, we propose a generalization of the algorithm that works for any case of the class polynomial (possibly having degree higher than two) associated to a special prime factor p of the input integer. Moreover, in contrast to the previous paper [25] which

dealt with only the case of primes $p = 1 + Dv^2$, we also point out that our algorithm can be similarly applied to the case where $p = t^2 + Dv^2$ $(t, v \in \mathbb{Z})$ such that $p + 1 - t$ is a smooth integer, that is, the biggest prime factor of $p+1-t$ is small. This further enlarges the possible choices of the prime factor p for which our proposed algorithm works efficiently.

Organization

This thesis consists of two parts and is organized as follows.

The first three chapters are devoted to the first work: the Diophantine problem of elliptic curves over function fields over $\mathbb{C}$. In Chapter 1, we summarize the basic theory of elliptic curves and explain our motivation for this work. Elliptic curves over $\mathbb{C}(t)$ are the main objects in this thesis. There is a correspondence between elliptic curves over $\mathbb{C}(t)$ and elliptic surfaces over $\mathbb{C}$ with the base curve $\mathbb{P}^1$. Thus in Chapter 2 we review the basic theory of elliptic surfaces and explain the correspondence. Via this correspondence, the Diophantine problem on elliptic curves over $\mathbb{C}(t)$ is translated into a problem of cohomology of elliptic surfaces. This allow us to utilize geometric methods for computing of the rank of elliptic curve over $\mathbb{C}(t)$. Moreover, we give a technical overview and comparison between our work and the known results. Chapter 3 is the main part of this thesis. We construct certain elliptic curves over $\mathbb{C}(t)$ and show that their rank growths in cyclotomic towers $\mathbb{C}(t^{\frac{1}{n}})/\mathbb{C}(t)$ is bounded independently on n.

The second work is described in Chapter 4. First, we revisit the basic theory of elliptic curves with emphasizing computational aspects and recall ECM and CM method. After that, we describe our proposed algorithm to factoring integers, which is efficient for composite numbers having a prime factor of special form.

Acknowledgements

First of all, I would like to express my gratitude to my supervisor, Prof. Masanori Asakura. I am grateful to him for longstanding film guidance and useful discussion. Without his support, I would not have accomplished the first work [1]. I am proud to get his direction in my graduate work. Moreover, I was supported by National Institute of Advanced Industrial Science and Technology (AIST) during the second work [2]. I also greatly appreciate this support. Finally, I would like to thank my parents and friends for help me during my life at Hokkaido University.

Contents

1 Elliptic Curves **8**
1.1 Definitions and Basic Theory 8
1.2 Motivation for the First Work 13

2 Elliptic Surfaces **15**
2.1 Definitions and Basic Properties 15
2.2 The Shioda's Isomorphism 18
2.3 Known Results on Problem 1.2.1 19

3 Main Results of the First Work **22**
3.1 Setting 22
3.2 Computation of the Cohomology 25
3.3 Proof of Proposition 3.2.5 32

4 Main Results of the Second Work **35**
4.1 Preliminaries for the Second Work 35
4.2 The Elliptic Curve Method 37
4.3 The Complex Multiplication Method 38
4.4 Setting 40
4.5 Our Proposed Algorithms 42

Chapter 1

Elliptic Curves

As mentioned in the introduction, this research is aimed at studying the Diophantine problem of elliptic curves over a function field over $\mathbb{C}$. In this chapter, for a background of our work, we start with a summary of the basic theory of elliptic curves and after that, state our problem in the thesis.

1.1 Definitions and Basic Theory

Let k be a field. In an arithmetic situation, a field k could be a number field, a finite field, a local field, a function field over the complex numbers or either of the former fields.

Definition 1.1.1. An elliptic curve E over k is defined to be a smooth projective curve of genus one over k, together with a distinguished k-rational point O. For any field extension k'/k, $E(k')$ denotes the set of k'-rational point of E. We write E/k instead of E for elliptic curves when we emphasize the base field k.

As is well known, every elliptic curve over $\mathbb{C}$ is a one dimensional torus as a Riemann surface; for some lattice $\Lambda \subset \mathbb{C}$,

$$E/\mathbb{C} \cong \mathbb{C}/\Lambda. \tag{1.1.1}$$

On the other hand, Riemann surfaces should have algebraic representation. In fact, we have an explicit description of elliptic curves by polynomials.

Proposition 1.1.2. *Let E be an elliptic curve over k with a distinguished k-rational point O. Then E is isomorphic to a smooth cubic curve in $\mathbb{P}^2$ over k given by an equation over k of the form:*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1.2}$$

and O corresponds to the point $(0:1:0) \in \mathbb{P}^2$. Moreover, if ch $k \neq 2, 3$, the above equation is transformed to:

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{1.1.3}$$

Proof. We can take a rational point $O \in E(k)$ since $E(k) \neq \phi$. We consider the divisor $3O$. For a divisor D, which is a formal sum of points on E, set $\mathfrak{L}(D) := \{f \in \overline{k}(E) \mid \mathrm{div}(f) \geq -D\}$ where $\overline{k}(E)$ denotes the function field of E over $\overline{k}$. Then, we have $\dim_{\overline{k}}\mathfrak{L}(3O) = 3$ by Riemann-Roch theorem. We can take a basis $\{1, x, y\}$ of $\mathfrak{L}(3O)$ over $\overline{k}$ such that x has a pole of order 2 at O and y has a pole of order 3 at O. We may assume that $x, y \in k(E)$ since E is defined over k. Define a morphism from E to $\mathbb{P}^2$ as follows:

$$\Phi_{|3O|} : E \to \mathbb{P}^2 \ ; \ P \mapsto (X : Y : Z) = (x(P) : y(P) : 1).$$

Then, we can see that it is an embedding i.e., $E \cong \Phi(E) \in \mathbb{P}^2$. Hence there is a homogeneous polynomial f which defines $\Phi(E)$ in $\mathbb{P}^2$ and by the genus formula we have $\deg(f) = 3$ since the genus of E is 1.

Moreover, when we consider the divisor $6O$ and $\mathfrak{L}(6O)$, we have $\dim_{\overline{k}}\mathfrak{L}(6O) = 6$. Then, by using elements $1, x, y, x^2, x^3, y^2, xy \in \mathfrak{L}(6O)$, we have a nontrivial relation with some $a_i, b_j \in k$:

$$a_0y^2 + a_1xy + a_2y = b_0x^3 + b_1x^2 + b_2x + b_3. \tag{1.1.4}$$

Since $\deg(f) = 3$, we conclude that

$$I(\Phi(E)) = (a_0Y^2Z + a_1XYZ + a_2YZ^2 - b_0X^3 - b_1X^2Z - b_2XZ^2 - b_3Z^3)$$

where the left side hand is the definite ideal of $\Phi(E)$ in $\mathbb{P}^2$.

Smoothness of E implies $a_0 \neq$ and $b_0 \neq 0$. We may assume that $a_0 \neq 0$ and $b_0 = 1$. By replacing $x,\ y$ with $a_0x,\ a_0y$ respectively, the equation 1.1.4 is transformed into:

$$y^2 + a_1'xy + a_2'y = x^3 + b_1'x^2 + b_2'x + b_3'.$$

Moreover, when we assume that the characteristic of k does not equal to 2 or 3, by replacing $x,\ y$ with $x + \frac{b_1'}{3}, y + \frac{a_1'}{2}x + \frac{a_2'}{3}$, we obtain:

$$y^2 = x^3 + ax + b,$$

and $\Phi(O) = (0 : 1 : 0)$. We can see easily that $\Phi(E)$ is smooth if and only if $4a^3 + 27b^2 \neq 0$. □

The equations of the form (1.1.2) are called the generalized Weierstrass equations. Conversely, every smooth cubic curve in $\mathbb{P}^2$ defined by a generalized Weierstrass equation over k is an elliptic curve over k.

Since we focus on elliptic curves over a field of characteristic 0, we take the equation of the form (1.1.3) as an equation of elliptic curves. When we put $Z = 0$ in an equation of the form (1.1.3), we obtain $(X : Y : Z) = (0 : 1 : 0) = O$. This means that there is only one point O on the line at infinity $\{Z = 0\} \subset \mathbb{P}^2$. We thus always regard O as a distinguished k-rational point and usually consider elliptic curves as the affine form;

$$y^2 = x^3 + ax + b,$$

which is simply called the Weierstrass form.

For the cubic curve defined by the Weierstrass equation $E : y^2 = x^3 + ax + b$, we define the discriminant Δ_E of E: $\Delta_E = -16(4a^3 + 27b^2)$. We recall that elliptic curves have to be smooth. As we have seen in the proof, E defines an elliptic curve if and only if $\Delta_E \neq 0$.

One of the most important problem in number theory is to study the solutions of algebraic equations over fields as mentioned at Introduction. Such problems are generally called the Diophantine problem [1]. From this point of view, the set;

$$E(k) = \{(x, y) \in k^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}.$$

is an important object in the research on the arithmetic of elliptic curves. So our problem is;

[1]The term "Diophantine problem" is often used for a system of equations with rational coefficients. In this thesis, without limiting problems to the case of rational coefficients, we use this term for a broader scope; number fields coefficients, function fields coefficients and so on.

Problem 1.1.3 (The Diophantine problem for elliptic curves)**.** *Let k be one of the fields mentioned at the beginning of this section. Study the set $E(k)$ for any elliptic curve E over k.*

More specifically, the above problem asks the number of solutions of elliptic curves, some structure on $E(k)$ and so on. But this problem is still unclear. In the following, we discuss the set $E(k)$ to make this problem more accurate.

Let us now see closely the properties of the set $E(k)$. The most fundamental property of elliptic curves is that the set of rational points carries the structure of an abelian group with the identity O. This leads the problem to be precise.

In order to explain this fact, we prepare some notation from the general theory of algebraic curves. For a smooth projective curve C over a field k, we set

$$\mathrm{Div}(C) := \{ \sum_{\text{finite}} n_i P_i \mid P_i \in C(\overline{k}) \ , \ n_i \in \mathbb{Z} \}.$$

This is an abelian group naturally and elements in $\mathrm{Div}(C)$ are called divisors on C. For rational functions $f \in \overline{k}(C)^{\times}$, we can associate to f the divisor $\mathrm{div}(f)$ given by $\mathrm{div}(f) := \sum_{P \in C} \mathrm{ord}_P(f) P$. In fact, this is a divisor since there are only finitely many points of C at which f has a pole or zero. For $D = \sum n_i P_i \in \mathrm{Div}(C)$, we define degree of D as $\sum n_i \in \mathbb{Z}$. We denote $\mathrm{Div}^0(C)$ the subgroup of $\mathrm{Div}(C)$ consisting of divisors of degree 0. Two divisors $D_1, D_2 \in \mathrm{Div}^0(C)$ are linearly equivalent if their difference is the divisor of a rational function, that is:

$$D_1 \sim D_2 \Leftrightarrow D_1 - D_2 = \mathrm{div}(f) \ \text{ for some } f \in \overline{k}(C) \setminus \{0\}.$$

We can see that this is an equivalence relation. Then,

$$\mathrm{Pic}^0(C) := \mathrm{Div}^0(C) / \sim$$

is also an abelian group. The class of $D \in \mathrm{Div}^0(C)$ is denoted by $[D] \in \mathrm{Pic}^0(C)$. We define $\mathrm{Div}_k(C)$ to be the subgroup of $\mathrm{Div}(C)$ consisting of $\mathrm{Gal}(\overline{k}/k)$-action invariant elements. Similarly, the linearly equivalence in $\mathrm{Div}_k(C)$ is defined by

$$D_1 \sim D_2 \Leftrightarrow D_1 - D_2 = \mathrm{div}(f) \ \text{ for some } f \in k(C) \setminus \{0\},$$

and we define

$$\mathrm{Pic}^0_k(C) := \mathrm{Div}^0_k(C)/\sim .$$

The following is the Abel-Jacobi theorem.

Theorem 1.1.4. *Let E be an elliptic curve over k with distinguished point O. Then, the maps $E(\bar{k}) \to \mathrm{Pic}^0(E); P \mapsto [P-O]$ and $E(k) \to \mathrm{Pic}^0_k(E); P \mapsto [P-O]$ induce bijections.*

This yields that elliptic curves and the set of rational points carry the structure of abelian group via the correspondence in Theorem 1.1.4.

Remark 1.1.5. In the above discussion, we define an abelian group structure on the set of rational points on an elliptic curve in an abstract way. Actually, there is well known an algebraic formula of the addition in $E(k)$. In particular, the operation of scalar multiplication plays a key role in the application of elliptic curves to cryptography. In §4, we see the formula of scalar multiplication and its application.

The following famous theorem is firstly shown in the case of elliptic curves over $\mathbb{Q}$ by Mordell [20]. Some years later Weil generalized it for abelian varieties over a number field [36].

Theorem 1.1.6 (Mordell-Weil theorem)**.** *Let k be a number field and E an elliptic curve over k. Then the group $E(k)$ is a finitely generated abelian group:*

$$E(k) \cong \mathbb{Z}^{\oplus r} \oplus E(k)_{tors}.$$

We refer to [28], [35] for the proof.

For the direction of our research, we are mainly concerned with elliptic curves over the function field of a curve. The function field analogue of Mordell-Weil theorem is the following.

Theorem 1.1.7 (Modell-Weil theorem for function fields)**.** *Let K be the function field of a curve over k and E/K an elliptic curve. If the j-invariant of E is non constant, then $E(K)$ is a finitely generated.*

For details, we refer to [26], Ch.III.

Hereafter, in this section, we assume that a base field k is either a number field or a function field.

The groups $E(k)$ are called the Mordell-Weil groups. We define the rank of E/k to be the rank of the abelian group $E(k)$. Thanks to the Mordell-Weil theorem, the rank is finite in the arithmetic situation in Theorem 1.1.6 and 1.1.7. For an elliptic curve E/k and a finite extension K/k, when we regard E/k as the elliptic curve over K naturally, the rank of $E(K)$ is also called the rank of E by abuse the notation.

Problem 1.1.8. *For given an elliptic curve over a number field or a function field, compute the rank and torsion part of $E(k)$.*

As we will remark the following soon, there is a decisive theorem on the torsion part of elliptic curves over $\mathbb{Q}$. On the other hand, in most cases, problems on the rank are hopelessly difficult and there are still lots of open problems to date. Later on, we compute the rank of elliptic curves over the function field $\mathbb{C}(t)$ under the some condition.

Remark 1.1.9. Besides the above problem, we can ask the question: Which groups arise as $E(k)$ for some elliptic curve E. As we allude above, for elliptic curves over $\mathbb{Q}$, the celebrated theorem by Mazur [18], [19] answers the question on the torsion part. On the other hand, it is even unknown that whether the rank is bounded when elliptic curves over $\mathbb{Q}$ are varied.

1.2 Motivation for the First Work

In this section, we formulate our problem presicely. Related works are discussed in §2.3.

Let k be a number field and p be a prime number. In [17], Mazur conjectured that, for the cyclotomic $\mathbb{Z}_p$-extension K/k and an elliptic curve over k with good reduction at p, the Mordell-Weil group $E(K)$ is finitely generated. We discuss a function field $\mathbb{C}(t)$ analogue of this conjecture. This is also a geometric analogue of the arithmetic of elliptic curves.

Problem 1.2.1. *Let $E/\mathbb{C}(t)$ be a elliptic curve. Then, in the cyclotomic towers of function fields $\mathbb{C}(t^{\frac{1}{n}})/\mathbb{C}(t)$, are the ranks of $E(\mathbb{C}(t^{\frac{1}{n}}))$ bounded independently on n?*

For a function field $\mathbb{F}_q(t)$ analogue, Shioda [23], Ulmer [32] constructed decisive answer. They constructed elliptic curves over $\mathbb{F}_q(t)$ with arbitrary

large rank. (We note that Shioda's example is isotrivial and Ulmer's one nonisotrivial.) We refer to [33] §4, for details of this direction.

On the other hand, there are several studies that give a rank bound for some function field extension of characteristic zero in terms of a conducter [27], [29], [11], [21].

Here, what we discuss in the thesis is the asymptotic behavior of rank growth of $E(\mathbb{C}(t^{\frac{1}{n}}))$ $(n = 1, 2, \cdots)$. For Problem 1.2.1, positive examples are constructed by Stiller [30] and Fastenberg [12], [13]. In this work, we present a new method for computing the rank of $E(\mathbb{C}(t^{\frac{1}{n}}))$ and construct new positive examples by exploiting this method. Our examples are essentially different from the previous ones.

Chapter 2

Elliptic Surfaces

In this chapter, we introduce elliptic surfaces and explain how these objects (over $\mathbb{C}$) correspond to elliptic curves (over the function field $\mathbb{C}(t)$). Via the correspondence, we see that the rank of the Mordell-Weil group $E(\mathbb{C}(t))$ are written by that of the Néron-Severi group of elliptic surface. This fact yields that we can exploit the Hodge theory to study the Modell-Weil group over $\mathbb{C}(t)$.

2.1 Definitions and Basic Properties

We start by defining elliptic surfaces.

Definition 2.1.1. Let k be an algebraically closed field and C a smooth projective curve over k. An elliptic surface $f : \mathcal{E} \to C$ is a smooth projective surface $\mathcal{E}$ over k with a surjective morphism satisfying the following consitions:

- almost all fibers are curves of genus 1 over k;
- all fibers not contains a (-1)-curve, which is a smooth rational curve with self-intersection number -1.

For the sake of simplicity, we often denote by $\mathcal{E}$ an elliptic surface $f : \mathcal{E} \to C$.

The fibers of f which are not smooth (i.e. has at least one singular point) are called singular fibers. A section of an elliptic curves $f : \mathcal{E} \to C$ is a

morphism $\pi : C \to \mathcal{E}$ such that $f \circ \pi = id_C$. The set of sections of f is denoted by $\mathcal{E}(C)$.

The singular fibers of an elliptic surface $\mathcal{E}$, as we will see later, have much information on $\mathcal{E}$. The type of reducible singular fibers are classified by Kodaira and he introduces the notation representing the type of fibers [15], Theorem6.2. We use his notation in the thesis. Moreover, he shows that the type is determined locally by the monodromy and computes the local monodromy matrices. The date on singular fibers which we need throughout the thesis are summarized in Table 2.1, see [15], Theorem9.1, Table I, or [5], Chapter V, Table 6.

Notation of the type of a fiber	the number of irreducible component	the monodromy matrix
I_0	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
I_n $(n \geq 1)$	n	$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
II	1	$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$
III	2	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
IV	3	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$
I_n^* $(n \geq 0)$	$n+5$	$-\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
II^*	9	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$
III^*	8	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
IV^*	7	$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$

Table 2.1: The type of singular fibers.

Here, I_0 denotes a smooth fiber. The type I_n is called multiplicative and the others are called additive.

We now state a relationship between elliptic curves over the function field of a smooth projective curve C/k and elliptic surfaces over k.

Theorem 2.1.2. *For k and C as above, let $K = k(C)$. Let (E, O) be an elliptic curve over K be the function field of C/k. Then, up to isomorphism, there is the unique elliptic surface $f : \mathcal{E} \to C$ with a section. Conversely, for an elliptic surface $f : \mathcal{E} \to C$ having at least one section, we obtain an elliptic curve E/K by taking the generic fiber of f. This correspondence is one-to-one and induces a bijection:*

$$E(K) \to \mathcal{E}(C);\ P = (x, y) \mapsto \big(\pi_P :\ t \mapsto (x(t), y(t), t)\big) \tag{2.1.1}$$

The section corresponding $O \in E(K)$ is called the zero section.

We give a rough discussion for the theorem. Let E be an elliptic curve over $K = k(C)$ defined by $y^2 = x^3 + a(t)x + b(t)$. For $t_0 \in C$, E_{t_0} denotes the cubic curve over k defined by $y^2 = x^3 + a(t_0)x + b(t_0)$. Then, except for the points $t_0 \in C$ such that E_{t_0} is singular (such point is called a bad place), they are elliptic curves over k. S denotes the set of bad places of C and we put $C^\circ := C \setminus S$. Then, E defines a surface $\mathcal{E}^\circ := \{(t, (X : Y : Z)) \mid Y^2Z = X^3 + a(t)XZ^2 + b(t)Z^3\} \subset C^\circ \times \mathbb{P}^2$ whose general fibers and the generic fiber are given by E_{t_0} and E respectively. Note here that $\mathcal{E}^\circ$ is equipped with $f' : \mathcal{E}^\circ \to C'$ via the projection $C' \times \mathbb{P}^2 \to \mathbb{C}^\circ$. Therefore, by taking the Zariski closure $\overline{\mathcal{E}}^\circ$ of $\mathcal{E}^\circ$ in $C \times \mathbb{P}^2$ and the minimal desingularization of $\overline{f}' : \overline{\mathcal{E}}^\circ \to C$, we obtain the surface $\mathcal{E}$ satisfying conditions in the statement. Uniqueness is followed by the relatively minimalness.

In general, elliptic surfaces do not necessarily have sections and singular fibers. We here employ the following assumption since those which we deal with here are equipped with these structure.

Assumption 2.1.3. All elliptic surfaces in the thesis have at least one section and singular fiber.

In the following, we identify elliptic curves over the function field of a curve C/k and elliptic surfaces over k with the base curve C by Theorem 2.1.2 under Assumption 2.1.3.

Moreover, since we are not concerned with a general base curve C, we only deal with the projective line $\mathbb{P}^1$ over $\mathbb{C}$ as a base curve of elliptic surfaces. Under the above conventions, from now on, we identify elliptic curves over $\mathbb{C}(t)$ with the corresponding elliptic surfaces $f : \mathcal{E} \to \mathbb{P}^1$.

Let E be a elliptic curve over $\mathbb{C}(t)$ and $\mathcal{E}$ the corresponding elliptic surface. Then, we can compute singular fibers of $\mathcal{E}$ using Tate's algorithm, which is so simple [31].

2.2 The Shioda's Isomorphism

This section is devoted to explain a relation between the Mordell-Weil group of an elliptic curve $E/\mathbb{C}(t)$ and the Nŕon-Severi group of the elliptic surface attached to E. Here, we concentrate on the facts that are needed later. For more detail and discussion of this section, we refer to [22] or [24].

We introduce some notation and terminology. Let $E/\mathbb{C}(t)$ be an elliptic curve and $f : \mathcal{E} \to \mathbb{P}^1$ the elliptic surface attached to $E/\mathbb{C}(t)$. Divisors on $\mathcal{E}$ is a finite formal sum of irreducible curves in $\mathcal{E}$: $D := \sum_i n_i \Gamma_i$ ($n_i \in \mathbb{Z}$, Γ_i: irreducible curves in $\mathcal{E}$). Divisors consisting of fiber components are called fibral divisors. The Néron-Severi group $NS(\mathcal{E})$ of $\mathcal{E}$ is defined to be the abelian group consisting of divisors on $\mathcal{E}$ modulo algebraic equivalence. Note that all fibers of f are algebraically equivalent. We identify sections with divisors defined by its image in $\mathcal{E}$. Via this identification, the one-to-one correspondence (2.1.1) shows that $\mathbb{C}(t)$-rational points of E give elements in $NS(\mathcal{E})$ and the divisor corresponding to $O \in E(\mathbb{C}(t))$ is called the zero divisor.

The following theorem translates problems on the Mordell-Weil group into those on the Néron-Severi group and allows us to utilize geometric methods for the Diophantine problem of elliptic curves over $\mathbb{C}(t)$.

Theorem 2.2.1 (Shioda,[24])**.** *Notation as above. Let T be the subgroup of $NS(\mathcal{E})$ generated by the zero section and fibral divisors. Then, we have*

$$E(\mathbb{C}(t)) \cong NS(\mathcal{E})/T,$$

and thus

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{C}(t)) = \mathrm{rank}_{\mathbb{Z}} NS(\mathbb{E}) - \mathrm{rank}_{\mathbb{Z}} T.$$

The rank of T is easy to compute by using Tate's algorithm. For $t \in \mathbb{P}^1$, we denote by E_t the fiber at t and by m_t the number of irreducible components of E_t. Set $S := \{\text{bad places}\} \subset \mathbb{P}^1$. Then, we have the following formula.

Proposition 2.2.2. *We have*

$$\mathrm{rank}_{\mathbb{Z}} T = 2 + \sum_{t \in S} (m_t - 1).$$

Thanks to the above isomorphism, one can utilize the Hodge theory for studying Modell-Weil group, namely the Lefschetz theorem on (1,1) classes ([34], Theorem7.2) implies the isomorphism:

$$E(\mathbb{C}(t)) \cong \big(H^2(\mathcal{E}, \mathbb{Z}) \cap H^{1,1}\big)/T \tag{2.2.1}$$

where, by abuse of notation, T denotes the image of $T \subset NS(\mathcal{E})$ under the cycle map $NS(\mathcal{E}) \to H^2(\mathcal{E}, \mathbb{Z})$.

2.3 Known Results on Problem 1.2.1

In this section, we give a technical overview of our work and compare our objects with the previous ones.

Here, recall that our direction is to construct elliptic curves over $\mathbb{C}(t)$ having a bounded rank in the cyclotomic tower $\mathbb{C}(t^{\frac{1}{n}})/\mathbb{C}(t)$. Stiller [30] and Fastenberg [12], [13] constructed positive examples for Problem 1.2.1. In Stiller's paper [30] §.5, elliptic curves over $\mathbb{C}(t)$ with bounded rank in the cyclotomic towers are exhibited. For example, the elliptic curve

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

has ranks over $\mathbb{C}(t^{\frac{1}{n}})$ as follows;

$$\mathrm{rk} E\big(\mathbb{C}(t^{\frac{1}{n}})\big) = \sum_{d|n, d=2,3,4,5} \phi(d), \tag{2.3.1}$$

where ϕ denotes the Euler function. We note that E degenerates at three points $t = 0, 1, \infty$ and the singular fibers of E_1 are multiplicative at $t = 0, 1$ and additive at $t = \infty$. Similarly, the ranks of the other examples are also written as a sum of the Euler functions.

On the other hand, Fastenberg [12] shows that, for an elliptic curve E over $\mathbb{C}(t)$ with certain conditions, the rank of $E(\mathbb{C}(t^{\frac{1}{n}}))$ is bounded independently on n. Moreover, the explicit upper bounds on the rank of $E(\mathbb{C}(t^{\frac{1}{n}}))$ for several examples are given in [13]. These upper bounds are written as a sum of the Euler functions with coefficients 1 just like Stiller's examples.

In this thesis, we give an explicit formula for the ranks of some elliptic curves over $\mathbb{C}(t)$ as follows;

$$E(\mathbb{C}(t^{\frac{1}{n}})) = \sum_{d|n, 1<d\leq d_{min}} 2\phi(d)$$

where d_{min} is a constant number defined by the type of singular fibers of E (see Proposition 3.2.2). For the detail of the formula, see Theorem 3.2.5. The difference between previous examples and our examples appears in the coefficients of the Euler function. A difficulty in the computation of the rank of our objects occurs from this.

For details, we now give a rough sketch of our strategy to compute the ranks. We consider $E/\mathbb{C}(t)$ be an elliptic curve and $f : \mathcal{E}_1 \to \mathbb{P}^1$ the elliptic surface attached to E. Let $\mathcal{E}_n$ be the elliptic surface obtained by pulling back $\mathcal{E}_1$ by the morphism $\mathbb{P}^1 \to \mathbb{P}^1;\ t \mapsto t^n$. Then, we have

$$E(\mathbb{C}(t^{\frac{1}{n}})) \cong NS(\mathcal{E}_n)/T_n \cong \left(H^2(\mathcal{E}_n, \mathbb{Z}) \cap H^{1,1}\right)/T_n$$

where T_n denote the subgroup of $NS(\mathcal{E}_n)$ generated by the zero section and fibral divisors. We now consider a $\mathbb{Q}$-Hodge structure $M_n := H^2(\mathcal{E}_n, \mathbb{Q})/(T_n \otimes \mathbb{Q})$ instead of the right hand side of the above isomorphisms. Then, we have to compute $\dim_{\mathbb{Q}} M_n \cap M^{1,1}$, where $M^{1,1} \subset M_n \otimes \mathbb{C}$ denotes the Hodge (1,1)-part of the Hosge structure M_n.

We observe that the elliptic surface $\mathcal{E}_n$ has an automorphism $\sigma : (x, y, t) \mapsto (x, y, \zeta_n t)$, where ζ_n denotes a primitive n-th root of unity. Thus M_n has a $\mathbb{Q}[\sigma]$-module structure. The central part of our computation is studying this structure. Define $L_n^d := \mathrm{Ker}(\Phi_d(\sigma) : M_n \to M_n)$ for a positive integer d which divides n, where $\Phi_d(x)$ denotes the minimal polynomial of $\mathbb{Q}(\zeta_d)$. Then, we have a decomposition of the Hodge structure

$$M_n = \bigoplus_{d|n} L_n^d.$$

Consequently, we can see that it suffices to compute $r_n^d := \dim_{\mathbb{Q}} L_n^d \cap L^{1,1}$ for $d \nmid n$, where $L^{1,1}$ denotes the Hodge (1,1) part of L_n^d.

In the previous studies, the case that the dimension of L_n^d as a $\mathbb{Q}(\zeta_d)$-vector space is one is discussed. This determines that the coefficients of Euler function in the formula (2.3.1) are one. These objects are obtained by putting various restrictions on the discriminant of elliptic curves over $\mathbb{C}(t)$. This affects the global structure of the corresponding elliptic surfaces like the Stiller's example as above. Since $L_n^d \cap L^{1,1}$ is a subspace of L_n^d, in order to compute l_n^d, we have only to determine whether the subspaces vanish or not. The present investigation, however, deal with the case that $\dim_{\mathbb{Q}(\zeta_d)} L_n^d = 2$. The difference is crucial since a new difficulty arises. In addition to the above problem, we need to compute either $l_n^d = 1$ or 2 if $L_n^d \cap L^{1,1}$ does not vanish. We overcome this difficulty by linking the monodromy of a fibration of elliptic surfaces with the monodromy of the Gaussian hypergeometric functions (see the key lemma: Lemma 3.3.1). Introducing this technique is the main contribution in this work. The monodromy of hypergeometric functions is well studied in [7]. Therefore, we apply this result to compute l_n^d via the key lemma: Lemma 3.3.1 (see Proposition 3.3.2) .

Chapter 3

Main Results of the First Work

This is the heart of the thesis. Firstly, we define elliptic curves over $\mathbb{C}(t)$ on which we focus. Secondly, we compute the cohomology of elliptic surfaces attached to these curves. Finally, we determine the Mordell-Weil ranks according to the strategy as in §2.3.

3.1 Setting

We fix the setting and notation.

Let $f : \mathcal{X} \to \mathbb{P}^1_u$ be an elliptic surface over $\mathbb{C}$ having multiplicative fibers at two points and an additive fiber at a point. Here, we denote by $\mathbb{P}^1_u$ the projective line with inhomogeneous coordinate u. We may assume that $\mathcal{X}$ has singular fibers at three points $\{0, 1, \infty\} \subset \mathbb{P}^1_u$ and has the singular fibers of type I_a (resp. I_b) at 0 (resp. 1), an additive fiber at ∞ by the assumption. The possible types of singular fibers of such elliptic surfaces are classified in [14] and summarized in the following Table 3.1.

For $\alpha \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ and $n \in \mathbb{N}$, let $\widetilde{f}_{\alpha,n} : \mathcal{X} \times_{\mathbb{P}^1_u} \mathbb{P}^1_{u_n} \to \mathbb{P}^1_u$ be the base change of f by the morphism $g_{\alpha,n} : \mathbb{P}^1_{u_n} \to \mathbb{P}^1_u;\ u \mapsto \alpha - u^n$, where $\mathbb{P}^1_{u_n}$ denotes the source of $g_{\alpha,n}$ with inhomogeneous coordinate u_n to distinguish $\mathbb{P}^1_u$. We define an elliptic surface $f_{\alpha,n} : \mathcal{X}_{\alpha,n} \to \mathbb{P}^1_{u_n}$ by the following diagram;

	Multiplicative fiber 1	Multiplicative fiber 2	Additive fiber
Type.1	I_1	I_1	II^*
Type.2	I_1	I_2	III^*
Type.3	I_1	I_3	IV^*
Type.4	I_1	I_4	I_1^*
Type.5	I_1	I_1	I_4^*
Type.6	I_2	I_2	I_2^*

Table 3.1: Possible combinations of singular fibers in this situation.

$$\begin{array}{ccccc} \mathcal{X}_{\alpha,n} & \xrightarrow{i} & \mathcal{X} \times_{\mathbb{P}^1_u} \mathbb{P}^1_{u_n} & \xrightarrow{pr} & \mathcal{X} \\ & \searrow^{f_{\alpha,n}} & \downarrow \widetilde{f_{\alpha,n}} \quad \square & & \downarrow f \\ & & \mathbb{P}^1_{u_n} & \xrightarrow[g_{\alpha,n}]{} & \mathbb{P}^1_u \end{array}$$

where i is the minimal desingularization and pr is the first projection. Then $\mathcal{X}_{\alpha,n}$ has the singular fibers at $(2n+1)$-points. The I_a-type appears at $u_n = \zeta_n^k \sqrt[n]{\alpha}$ and the I_b-type appears at $u_n = \zeta_n^k \sqrt[n]{\alpha - 1}$ for $k = 0, 1, \cdots, n-1$, where we fix $\zeta_n := \exp(\frac{2\pi i}{n})$ from now on. The following Tables 3.2-3.5 collect the variation of singular fibers at ∞ depending on the index n of the above base change. These follow from the computation of local monodromy matrix, see Table 2.1.

$n \mod 6$	the type of fiber
1	II^*
2	IV^*
3	I_0^*
4	IV
5	II
0	I_0

Table 3.2: The type of $f_{\alpha,n}^{-1}(\infty)$ in $\mathcal{X}_{\alpha,n}$ of Type.1.

$n \mod 4$	the type of fiber
1	III^*
2	I_0^*
3	III
0	I_0

Table 3.3: The type of $f_{\alpha,n}^{-1}(\infty)$ in $\mathcal{X}_{\alpha,n}$ of Type.2.

$n \mod 3$	the type of fiber
1	IV^*
2	IV
0	I_0

Table 3.4: The type of $f_{\alpha,n}^{-1}(\infty)$ in $\mathcal{X}_{\alpha,n}$ of Type.3.

$n \mod 2$	the type of fiber
1	I_{nm}^*
0	I_{nm}

Table 3.5: The type of $f_{\alpha,n}^{-1}(\infty)$ in $\mathcal{X}_{\alpha,n}$ of Type.4.5.6.

For further discussion, we prepare several notation. Let $Z_{\alpha,n} := \big(f_{\alpha,n}^{-1}(0) + f_{\alpha,n}^{-1}(\infty) + \sum_{k=1}^{n-1}(f_{\alpha,n}^{-1}(\zeta_n^k \sqrt[n]{\alpha}) + f_{\alpha,n}^{-1}(\zeta_n^k \sqrt[n]{\alpha - 1}))\big)_{red}$ be the reduced divisor on $\mathcal{X}_{\alpha,n}$ and $U_{\alpha,n} \subset \mathcal{X}_{\alpha,n}$ the inverse image of $\mathbb{P}^1_u \setminus \{0, 1, \alpha, \infty\}$ via $g_{\alpha,n} \circ f_{\alpha,n}$. Moreover, set $\mathcal{S}_{\alpha,n} := \mathbb{P}^1_{u_n} \setminus \{u_n^n = 0, \alpha, \alpha - 1, \infty\}$. We denote by $E_{\alpha,n}$ the generic fiber of $f_{\alpha,n}$. According to the Mordell-Weil theorem for function fields (Theorem 1.1.7), the Mordell-Weil group $E_{\alpha,1}(\mathbb{C}(u_1^{\frac{1}{n}}))$ is a finitely generated abelian group. We will study the rank of the finitely generated abelian groups $E_{\alpha,1}(\mathbb{C}(u_1^{\frac{1}{n}}))$.

Hereafter, we denote u_1 by t and u_n by s. In the above setting, we have

$$E_{\alpha,1}\big(\mathbb{C}(t^{\frac{1}{n}})\big) \cong E_{\alpha,n}\big(\mathbb{C}(s)\big).$$

By Shioda's isomorphism (Theorem 2.2.1), we obtain

$$E_{\alpha,n}\big(\mathbb{C}(s)\big) \cong NS(\mathcal{X}_{\alpha,n})/T_{\alpha,n}.$$

3.2 Computation of the Cohomology

The elliptic surface $\mathcal{X}_{\alpha,n}$ has an automorphism σ given by $(x, y, s) \mapsto (x, y, \zeta_n s)$. In this section, we study the structure of the cohomology of elliptic surface $\mathcal{X}_{\alpha,n}$ as $\mathbb{Q}[\sigma]$-module. This is the first step toward the main theorem, that is, the bound of the rank of Mordell-Weil group of elliptic curve $E_{\alpha,1}$.

Set

$$\begin{aligned} M_{\alpha,n} &:= H^2(\mathcal{X}_{\alpha,n}, \mathbb{Q})/T_{\alpha,n,\mathbb{Q}} \\ &\cong W_2H^1(\mathcal{S}_{\alpha,n}, j^*R^1(f_{\alpha,n})_*\mathbb{Q}) \end{aligned}$$

where $j : \mathcal{S}_{\alpha,n} \hookrightarrow \mathbb{P}^1_s$ is the embedding. In this section, we study the structure of this module. Note that $M_{\alpha,n}$ is a $\mathbb{Q}$-Hodge structure on account of the inclusion $T_{\alpha,n,\mathbb{Q}} \subset H^2(\mathcal{X}_{\alpha,n}, \mathbb{Q}) \cap H^{1,1}$ endowed with multiplication by $\mathbb{Q}[\sigma]$.

Proposition 3.2.1. *We have*

$$\dim_{\mathbb{Q}} M_{\alpha,n} = \begin{cases} 2n-2 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is additive;} \\ 2n-3 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is multiplicative;} \\ 2n-4 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is smooth.} \end{cases}$$

Note that right hand side are not negative since for $n = 1$ the first case appear.

Proof. We have an exact sequence

$$0 \to H^1(\mathcal{S}_{\alpha,n}, j^*R^1(f_{\alpha,n})_*\mathbb{Q}) \to H^2(U_{\alpha,n}, \mathbb{Q}) \to H^2(\mathcal{X}_{\alpha,n,s}, \mathbb{Q})$$

where $\mathcal{X}_{\alpha,n,s}$ is a smooth general fiber of $f_{\alpha,n}$. By taking the graded piece of weight 2, we have an isomorphism

$$W_2H^1(\mathcal{S}_{\alpha,n}, j^*R^1(f_{\alpha,n})_*\mathbb{Q}) \cong \mathrm{Ker}\big(W_2H^2(U_{\alpha,n}, \mathbb{Q}) \to H^2(\mathcal{X}_{\alpha,n,s}, \mathbb{Q})\big). \quad (3.2.1)$$

Note that $H^2(\mathcal{X}_{\alpha,n,s}, \mathbb{Q}) \simeq \mathbb{Q}$ and the arrow in the right hand side is surjective. Hence

$$\dim_{\mathbb{Q}} M_{\alpha,n} = \dim_{\mathbb{Q}} W_2H^2(U_{\alpha,n}, \mathbb{Q}) - 1. \quad (3.2.2)$$

The localization exact sequence induces the following:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Coker}(H^2_{Z_{\alpha,n}}(\mathcal{X}_{\alpha,n}) \to H^2(\mathcal{X}_{\alpha,n})) & \longrightarrow & H^2(U_{\alpha,n}) & \longrightarrow & H^3_{Z_{\alpha,n}}(\mathcal{X}_{\alpha,n}) & \longrightarrow & H^3(\mathcal{X}_{\alpha,n}) \\ & & \cong\downarrow & & & & \| & & \| \\ & & W_2H^2(U_{\alpha,n}) & & & & H_1(Z_{\alpha,n}) & & 0. \end{array} \quad (3.2.3)$$

Here, all objects in the above diagram are with rational coefficient. Recall that $Z_{\alpha,n} = \left(f_{\alpha,n}^{-1}(0) + f_{\alpha,n}^{-1}(\infty) + \sum_{k=1}^{n-1}(f_{\alpha,n}^{-1}(\zeta_n^k \sqrt[n]{\alpha}) + f_{\alpha,n}^{-1}(\zeta_n^k \sqrt[n]{\alpha-1}))\right)_{red}$ where $f_{\alpha,n}^{-1}(0)$ is smooth, $f_{\alpha,n}^{-1}(\zeta_n^k \sqrt[n]{\alpha})$ and $f_{\alpha,n}^{-1}(\zeta_n^k \sqrt[n]{\alpha-1})$ are multiplicative for $k = 1, \cdots, n-1$. The fiber $f_{\alpha,n}^{-1}(\infty)$ depends on n, according to the table in §.2. Thus we obtain

$$\dim_{\mathbb{Q}} H_1(Z_{\alpha,n}, \mathbb{Q}) = \begin{cases} 2n+2 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is additive;} \\ 2n+3 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is multiplicative;} \\ 2n+4 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is smooth.} \end{cases}$$

Moreover, the Leray spectral sequence gives an exact sequence

$$\begin{aligned} 0 &\to H^1(S_{\alpha,n}, j^*R^1(f_{\alpha,n})_*\mathbb{Q}) \to H^2(U_{\alpha,n}, \mathbb{Q}) \\ &\to H^0(S_{an}, j^*R^2(f_{\alpha,n})_*\mathbb{Q}) \cong H^2(\mathcal{X}_{\alpha,n,t}, \mathbb{Q})^{\pi_1(\mathcal{S}_{\alpha,n})}. \end{aligned} \tag{3.2.4}$$

Note that the last term is one dimensional and the last arrow is surjection. Employing the formula

$$\chi(\mathcal{S}_{\alpha,n}, j^*R^1(f_{\alpha,n})_*\mathbb{Q}) = \chi(\mathcal{S}_{\alpha,n}, \mathbb{Q}) \times \mathrm{rank} j^*R^1(f_{\alpha,n})_*\mathbb{Q},$$

we have

$$\dim H^1(\mathcal{S}_{\alpha,n}, j^*R^1(f_{\alpha,n})_*\mathbb{Q}) = 4n.$$

Hence by (3.2.4)

$$\dim H^2(U_{\alpha,n}, \mathbb{Q}) = 4n+1$$

and so by (3.2.3)

$$\dim_{\mathbb{Q}} W_2H^2(U_{\alpha,n}, \mathbb{Q}) = \begin{cases} 2n-1 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is additive;} \\ 2n-2 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is multiplicative;} \\ 2n-3 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is smooth.} \end{cases}$$

We reach a conclusion by (3.2.2). □

Here, let $\sigma : \mathcal{X}_{\alpha,n} \to \mathcal{X}_{\alpha,n}$ be an automorphism given by $(x, y, s) \mapsto (x, y, \zeta_n s)$. Then, $\mathbb{Q}[\sigma]$ acts on $M_{\alpha,n}$. We will determine the structure of $M_{\alpha,n}$ as $\mathbb{Q}[\sigma]$-module.

For a positive integer d which divides n, we set

$$L^d_{\alpha,n} := \mathrm{Ker}\big(\Phi_d(\sigma) : M_{\alpha,n} \to M_{\alpha,n}\big)$$

where $\Phi_d(X)$ is the minimal polynomial of ζ_d over $\mathbb{Q}$. We have a decomposition

$$M_{\alpha,n} = \bigoplus_{d|n} L^d_{\alpha,n}.$$

of the Hodge structures. Then, we have

$$\begin{aligned} \mathrm{rank}E_{\alpha,1}\big(\mathbb{C}(t^{\frac{1}{n}})\big) &= \mathrm{rank}E_{\alpha,n}\big(\mathbb{C}(s)\big) \\ &= \dim_{\mathbb{Q}} M_{\alpha,n} \cap H^{1,1} \\ &= \sum_{d|n} \dim_{\mathbb{Q}} L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1}. \end{aligned} \tag{3.2.5}$$

Proposition 3.2.2. *Let d_{min} be the minimal integer such that the fiber $f^{-1}_{\alpha,d_{min}}(\infty)$ in $\mathcal{X}_{\alpha,d_{min}}$ is smooth or multiplicative. According to the Tables 3.2-3.5, if the elliptic surface $\mathcal{X}$ is Type.1 (resp. 2,3,otherwise) in Table 3.1, then $d_{min} =$ 6 (resp. $4, 3, 2$). Then, we have*

$$L^d_{\alpha,n} \cong \begin{cases} 0 & \text{if } d = 1 \\ \mathbb{Q}[\sigma]/\big(\Phi_d(\sigma)\big) & \text{if } d = d_{min} \\ \mathbb{Q}[\sigma]/\big(\Phi_d(\sigma)\big)^{\oplus 2} & \text{if } d \neq 1, d_{min} \end{cases}$$

as $\mathbb{Q}[\sigma]$-module.

Proof. We use induction on n. Write $n = ml$ where m, l are positive integers. Then we have an unramified cyclic covering

$$\pi_l : U_{\alpha,n} \to U_{\alpha,m} \ ; \ (x, y, u_n) \mapsto (x, y, u_n^l)$$

and this induces an injection

$$\pi_l^* : M_{\alpha,m} \hookrightarrow M_{\alpha,n}.$$

Via the above injection, since $U_n/\langle\sigma^m\rangle \cong U_m$, we obtain an isomorphism

$$M_{\alpha,m} \xrightarrow{\cong} M^{\sigma^m=1}_{\alpha,n} \tag{3.2.6}$$

where $M_{\alpha,n}^{\sigma^m=1}$ denotes the subspace of $M_{\alpha,n}$ consisting of elements on which σ^m acts trivially. Moreover, $\pi_l^*(L_{\alpha,m}^d) \subset L_{\alpha,n}^d$ for $d \mid m \mid n$. By the isomorphism (3.2.6), we have

$$L_{\alpha,m}^d \cong (L_{\alpha,n}^d)^{\sigma^m=1} = L_{\alpha,n}^d \text{ for } d \mid m \mid n.$$

Here the second equality follows from the fact that $\Phi_d(\sigma)$ divides $\sigma^m - 1$. We sum up the above discussion in the following diagram:

$$\begin{array}{ccc} & & M_{\alpha,n} \\ & & \cup \\ L_{\alpha,n}^d = (L_{\alpha,n}^d)^{\sigma^m=1} & \hookrightarrow & M_{\alpha,n}^{\sigma^m=1} \\ \cong\uparrow & & \cong\uparrow \pi_l^* \\ L_{\alpha,m}^d & \hookrightarrow & M_{\alpha,m} \end{array}$$

Put $l_{\alpha,n}^d := \dim_{\mathbb{Q}} L_{\alpha,n}^d$, then $\dim_{\mathbb{Q}} M_{\alpha,n} = \sum_{d|n} l_{\alpha,n}^d$. The above diagram yields $l_{\alpha,n}^d = l_{\alpha,m}^d$ for $d \mid m \mid n$. In particular, $l_{\alpha,n}^1 = l_{\alpha,1}^1 = 0$ by Proposition 3.2.1. And for $n = d_{min}$, we have by induction

$$\begin{aligned} \sum_{d|d_{min}} l_{\alpha,d_{min}}^d &= l_{\alpha,d_{min}}^{d_{min}} + 2 \sum_{d|d_{min}, d\neq 1, d_{min}} \phi(d) \\ &= \begin{cases} 2n-3 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is multiplicative i.e. } d_{min} = 2; \\ 2n-4 & \text{if } f_{\alpha,n}^{-1}(\infty) \text{ is smooth i.e. } d_{min}\text{=3 or 4 or 6.} \end{cases} \end{aligned}$$

Thus we obtain $l_{\alpha,d_{min}}^{d_{min}} = \phi(d_{min})$. Here, ϕ denotes the Euler function.

For general n, we similarly have

$$\sum_{d|n, d\neq 1} l_{\alpha,n}^d = \begin{cases} l_{\alpha,n}^n + 2 \sum_{d|n, d\neq 1, n} \phi(d) & \text{if } d_{min} \nmid n; \\ l_{\alpha,n}^n + \phi(d_{min}) + 2 \sum_{d|n, d\neq 1, d_{min}, n} \phi(d) & \text{if } d_{min} \mid n. \end{cases}$$

If d_{min} not divides n, the fiber $f_{\alpha,n}^{-1}(\infty)$ is additive. Then, we have

$$\dim_{\mathbb{Q}} M_{\alpha,n} = l_{\alpha,n}^n + 2 \sum_{d|n, d\neq 1, n} \phi(d) = 2n - 2.$$

Hence $l^n_{\alpha,n} = 2\phi(n)$. If d_{min} divides n and $f^{-1}_{\alpha,n}(\infty)$ is multiplicative, then $\phi(d_{min}) = 1$ and

$$\dim_{\mathbb{Q}} M_{\alpha,n} = l^n_{\alpha,n} + \phi(2) + 2 \sum_{d|n, d\neq 1, d_{min}, n} \phi(d) = 2n - 3.$$

and hence $l^n_{\alpha,n} = 2\phi(n)$. Finally, if d_{min} divides n and $f^{-1}_{\alpha,n}(\infty)$ is smooth, then $\phi(d_{min}) = 2$ and we conclude $l^n_{\alpha,n} = 2\phi(n)$ in the same way. We finish the proof. □

By the Proposition 3.2.2, the dimensions of the subspaces $L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1}$ over $\mathbb{Q}(\zeta_d)$ are at most 2. In the following, we will determine the dimension completely under the assumption that α is a transcendental number.

Firstly, we treat the case that $d \leq d_{min}$. This case can be computed as follows.

Proposition 3.2.3. *Let d_{min} be an integer as in Proposition 3.2.2. Then, if $d \leq d_{min}$, we have $L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1} = L^d_{\alpha,n}$.*

Proof. The assertion is equivalent to $(l^d_{\alpha,n})^{2,0} := \dim_{\mathbb{Q}}(L^d_{\alpha,n})^{2,0} = 0$. We denote the number of irreducible components of the fiber $f^{-1}_{\alpha,n}(s)$ by m_s. The Euler number $e\big(f^{-1}_{\alpha,n}(s)\big)$ of the fiber $f^{-1}_{\alpha,n}(s)$ are given by

$$e\big(f^{-1}_{\alpha,n}(s)\big) = \begin{cases} 0 & \text{if } f^{-1}_{\alpha,n}(s) \text{ is smooth;} \\ m_s & \text{if } f^{-1}_{\alpha,n}(s) \text{ is multiplicative;} \\ m_s + 1 & \text{if } f^{-1}_{\alpha,n}(s) \text{ is additive.} \end{cases} \tag{3.2.7}$$

The Hodge number of (2,0)-part is given by the Euler numbers of fibers:

$$h^{2,0}_n := \dim_{\mathbb{Q}} H^{2,0}(\mathcal{X}_{\alpha,n}) = -1 + \frac{1}{12} \sum_{s\in\mathbb{P}^1_s} e\big(f^{-1}_{\alpha,n}(s)\big). \tag{3.2.8}$$

By the Tables 3.1-3.5 and (3.2.7), (3.2.8),

$$h^{2,0}_n = \lfloor \frac{n-1}{d_{min}} \rfloor \tag{3.2.9}$$

where, for a real number r, $\lfloor r \rfloor$ denotes the maximum of integers which are smaller than or equal to r.

If $d \leq d_{min}$, we have $h^{2,0}_d = 0$ by (3.2.9). Thus, since $(l^d_{\alpha,d})^{2,0} = (l^d_{\alpha,n})^{2,0}$, we have $(l^d_{\alpha,n})^{2,0} = 0$. □

Secondly, we will prove that $L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1} = 0$ for $d > d_{min}$. In order to prove this, we set $S := \mathbb{P}^1 \setminus \{0, 1, \infty\}$ and consider a smooth fibration: $X \to S$ such that the fiber of $\alpha \in S$ is the elliptic surface $\mathcal{X}_{\alpha,n}$. Since $\pi_1(S, \alpha)$-action commutes with σ-action, the monodromy action on the cohomology of $\mathcal{X}_{\alpha,n}$ induces $\pi_1(S, \alpha)$-action on $L^d_{\alpha,n}$.

Proposition 3.2.4. *Suppose that α is a transcendental number. If $\dim_{\mathbb{Q}(\zeta_d)} L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1} \neq 0$, then $\pi_1(S, \alpha)$-action on $L^d_{\alpha,n}$ factors trough a finite quotient. In other wards,*

$$\mathrm{Im}\big(\pi_1(S, \alpha) \to \mathrm{Aut}(L^d_{\alpha,n})\big)$$

is a finite group.

Proof. Throughout this proof, all of the fundamental groups are considered with fixed base point $\alpha \in S$ and we omit to write the base point. Take a model $X_{\overline{\mathbb{Q}}}$ of X over $\overline{\mathbb{Q}}$. Consider the following cartesian diagram

$$\begin{array}{ccc} X_{\overline{\mathbb{Q}}} & \longrightarrow & S_{\overline{\mathbb{Q}}} := \mathrm{Spec}\overline{\mathbb{Q}}[T, \frac{1}{T}, \frac{1}{1-T}] \\ \uparrow & & \uparrow \\ Y := \mathcal{X}_{\alpha,n} \times_{\mathbb{C}} \mathrm{Spec}\overline{\mathbb{Q}}(T) & \longrightarrow & \mathrm{Spec}\overline{\mathbb{Q}}(T) \\ \uparrow & & \uparrow \\ \mathcal{X}_{\alpha,n} & \longrightarrow & \mathrm{Spec}\mathbb{C} \end{array}$$

where the morphism $\mathrm{Spec}\mathbb{C} \to \mathrm{Spec}\overline{\mathbb{Q}}(T)$ is induced by the morphism $\overline{\mathbb{Q}}(T) \to \mathbb{C}$; $T \mapsto \alpha$ (here we use the assumption that α is a transcendental number). Let $Y_{\overline{\mathbb{Q}(T)}} := Y \times_{\overline{\mathbb{Q}}(T)} \mathrm{Spec}\overline{\mathbb{Q}(T)}$. Since $NS(\mathcal{X}_{\alpha,n}) \cong NS(Y_{\overline{\mathbb{Q}(T)}})$, one has the isomorphism

$$L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1} \cong \Big(NS(Y_{\overline{\mathbb{Q}(T)}})/T_{\alpha,n}\Big) \cap \mathrm{Ker}\big(\Phi_{\mathrm{d}}(\sigma) : \mathrm{M}_{\alpha,\mathrm{n}} \to \mathrm{M}_{\alpha,\mathrm{n}}\big),$$

and hence the Galois group $\mathrm{Gal}\big(\overline{\mathbb{Q}(T)}/\overline{\mathbb{Q}}(T)\big)$ acts on this. Since the Néron-Severi group of $\mathcal{X}_{\alpha,n}$ is finitely generated and the action of the Galois group on each cycles factors through a finite quotient, we have

$$\mathrm{Gal}\big(K/\overline{\mathbb{Q}}(T)\big) \to \mathrm{Aut}(L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1})$$

for some finite extension K of $\overline{\mathbb{Q}}(T)$. This completes the proof in the case $L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1} = L^d_{\alpha,n}$.

Suppose $L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1} \neq L^d_{\alpha,n}$, namely $\dim_{\mathbb{Q}(\zeta_d)}(L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1}) = 1$. Then there is the orthogonal decomposition

$$L^d_{\alpha,n} = (L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1}) \oplus (L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1})^{\perp}$$

with respect to polarization on $L^d_{\alpha,n}$ and $\pi_1(S')$ acts on each component, where S' is a smooth model of K. There is a $\mathbb{Z}$-lattice in each component induced from the $\mathbb{Z}$-lattice $H^2(\mathcal{X}_{\alpha,n}, \mathbb{Z})$ in $M_{\alpha,n}$, and $\pi_1(S')$ acts on it. Therefore, the image of $\pi_1(S')$ to $\mathrm{Aut}(L^d_{\alpha,n})$ is contained in $\mathbb{Z}^\times \times \mathbb{Z}^\times = \{\pm 1\} \times \{\pm 1\}$. In particular, it is finite. Thus a diagram

$$\begin{array}{ccc} \pi_1(S') & \longrightarrow & \mathrm{Aut}(L^d_{\alpha,n}) \\ \downarrow & \nearrow & \\ \pi_1(S) & & \end{array}$$

concludes the desired assumption. □

We postpone the proof of the following proposition to the next section.

Proposition 3.2.5. *For $d > d_{min}$,*

$$\mathrm{Im}\big(\pi_1(S, \alpha) \to \mathrm{Aut}(L^d_{\alpha,n})\big)$$

is an infinite group.

By Proposition 3.2.3, 3.2.4 and 3.2.5, we have the main theorem of this thesis, the explicit ranks of the Mordell-Weil group.

Theorem 3.2.6. *Suppose that α is a transcendental number. We have*

$$\begin{aligned} \mathrm{rank} E_{\alpha,1}(\mathbb{C}(t^{\frac{1}{n}})) &= \sum_{1<d\leq d_{min}, d|n} \dim_{\mathbb{Q}} L^d_{\alpha,n} \cap (L^d_{\alpha,n})^{1,1} \\ &= \begin{cases} \displaystyle\sum_{1<d<d_{min}, d|n} 2\phi(d) & \text{if } d_{min} \nmid n; \\ \displaystyle\sum_{1<d<d_{min}, d|n} 2\phi(d) + \phi(d_{min}) & \text{if } d_{min} \mid n. \end{cases} \end{aligned}$$

where ϕ denotes the Euler function.

3.3 Proof of Proposition 3.2.5

In this section, we will give the proof of Proposition 3.2.5. We assume that $d > d_{min}$ throughout this section.

Recall

$$M_{\alpha,n} = \bigoplus_{d\neq 1, d|n} L^d_{\alpha,n}$$

and

$$L^d_{\alpha,n} \cong \mathbb{Q}[\sigma]/\big(\Phi_d(\sigma)\big)^{\oplus 2} \qquad \text{if } d \neq 1, d_{min} \tag{3.3.1}$$

as $\mathbb{Q}[\sigma]$-modules. If we write $L^d_{\alpha,n,\mathbb{C}} := L^d_{\alpha,n} \otimes \mathbb{C}$, we have

$$L^d_{\alpha,n,\mathbb{C}} = \bigoplus_{\chi} L^d_{\alpha,n}(\chi)$$

where χ runs through the set of homomorphisms from $\mathbb{Q}(\zeta_d)$ to $\overline{\mathbb{Q}}$ and $L^d_{\alpha,n}(\chi)$ are the spaces of eigenvectors of σ with $\pi_1(S,\alpha)$-action. By (3.3.1), the spaces $L^d_{\alpha,n}(\chi)$ are two-dimensional over $\mathbb{C}$. In order to prove Proposition 3.2.5, it suffices to find an eigen component whose monodromy group is infinite.

Hereafter, we fix χ to be the homomorphism $\chi(\zeta_d) = \zeta_d$. Moreover we fix rational numbers $\lambda_1, \lambda_2 \in \mathbb{Q}$ such that $\exp(2\pi i\lambda_j)(j = 1, 2)$ and $\lambda_1 \leq \lambda_2$ are eigenvalues of the local monodromy on $\overline{\mathbb{Q}} \otimes_{\chi,\mathbb{Q}(\zeta_d)} R^1 f_* \mathbb{Q}$ where $f : \mathcal{X} \to \mathbb{P}^1$ as in the begining of § 3.1. Since the local monodromy of elliptic surfaces over $\mathbb{C}$ is completely classified, see Tabel 2.1, from the Table 3.1, we can list all of pairs (λ_1, λ_2) as in Table 3.6.

Table 3.6: Type of $\mathcal{X}$ and d_{min}, the pair (λ_1, λ_2).

Type of $\mathcal{X}$ in Table 3.1	d_{min}	(λ_1, λ_2)
Type.1	6	$\left(\frac{1}{6}, \frac{5}{6}\right)$
Type.2	4	$\left(\frac{1}{4}, \frac{3}{4}\right)$
Type.3	3	$\left(\frac{1}{3}, \frac{2}{3}\right)$
Type.4	2	$\left(\frac{1}{2}, \frac{1}{2}\right)$
Type.5	2	$\left(\frac{1}{2}, \frac{1}{2}\right)$
Type.6	2	$\left(\frac{1}{2}, \frac{1}{2}\right)$

In order to see the structure of $L^d_{\alpha,n}(\chi)$ as $\mathbb{C}[\pi_1(S,\alpha)]$-module, we make use of the Gaussian hypergeometric function.

Lemma 3.3.1. *Put* ${}_2F_1(x) := {}_2F_1\left(\begin{smallmatrix}\lambda_1-\frac{1}{d},\lambda_2-\frac{1}{d}\\ 1-\frac{1}{d}\end{smallmatrix};x\right)$ *the Gaussian hypergeometric functions. Let* V_α *to be two dimensional vector space over* $\mathbb{C}$ *spanned by* ${}_2F_1(\alpha)$ *and* ${}_2F_1(1-\alpha)$*, on which* $\pi_1(S,\alpha)$ *acts in the natural way. Then there is an isomorphism*

$$V_\alpha \cong L^d_{\alpha,n}(\chi)^\vee$$

of $\mathbb{C}[\pi_1(S,\alpha)]$*-modules where* $L^d_{\alpha,n}(\chi)^\vee$ *denotes the dual space.*

Proof. Recall $U_{\alpha,n} = (g_{\alpha,n}\circ f_{\alpha,n})^{-1}(\mathbb{P}^1\backslash\{0,1,\infty\})$ as in § 3.1. Put $H^2(U_{\alpha,n})_0 := \mathrm{Ker}\big(H^2(U_{\alpha,n}) \to H^2(\mathcal{X}_{\alpha,n,s})\big)$ where $\mathcal{X}_{\alpha,n,s}$ is a general smooth fiber. There is a natural isomorphism

$$W_2H^2(U_{\alpha,n})_0 \cong H^2(\mathcal{X}_{\alpha,n})/T_{\alpha,n} = M_{\alpha,n}$$

and this yields

$$\overline{\mathbb{Q}} \otimes_{\chi,\mathbb{Q}(\zeta_d)} W_2H^2(U_{\alpha,n})_0 \cong L^d_{\alpha,n}(\chi).$$

We employ [3] Theorem 4.1(period formula). There are two homology cycles $\Gamma_1,\Gamma_2 \in H_2(U_{\alpha,n},\overline{\mathbb{Q}})$ which form a basis of $\overline{\mathbb{Q}} \otimes_{\chi,\mathbb{Q}(\zeta_d)} H_2(U_{\alpha,n},\mathbb{Q})$, and two global rational forms $\omega_1,\omega_2 \in \Gamma(U_{\alpha,n},\Omega^2)$ which form a basis of $\overline{\mathbb{Q}} \otimes_{\chi,\mathbb{Q}(\zeta_d)} W_2H^2_{\mathrm{dR}}(U_{\alpha,n}/\mathbb{Q})_0$, and a differential operator Θ on $\overline{\mathbb{Q}}[\alpha]$ such that

$$\begin{pmatrix}\int_{\Gamma_1}\omega_1 & \int_{\Gamma_2}\omega_1\\ \int_{\Gamma_1}\omega_2 & \int_{\Gamma_2}\omega_2\end{pmatrix} = \begin{pmatrix}a_1G_1(\alpha) & a_2G_2(\alpha)\\ a_1G_1'(\alpha) & a_2G_2'(\alpha)\end{pmatrix}$$

for some constants $a_i \in \mathbb{C}^\times$ where we put $G_1(\alpha) := \Theta\big({}_2F_1(\alpha)\big)$ and $G_2(\alpha) := \Theta\big({}_2F_1(1-\alpha)\big)$. Note that the fact that the space $L^d_{\alpha,n}(\chi)$ is two-dimensional implies that the spaces $\overline{\mathbb{Q}}\otimes_{\chi,\mathbb{Q}(\zeta_d)} H_2(U_{\alpha,n},\mathbb{Q})$ and $\overline{\mathbb{Q}}\otimes_{\chi,\mathbb{Q}(\zeta_d)} W_2H^2_{\mathrm{dR}}(U_{\alpha,n}/\mathbb{Q})_0$ are two-dimensional. Moreover, the above matrix is invertible. This means that the composition

$$\mathbb{C}\Gamma_1 \oplus \mathbb{C}\Gamma_2 \longrightarrow H_2(U_{\alpha,n},\mathbb{C}) \longrightarrow W_2H^2_{\mathrm{dR}}(U_{\alpha,n}/\mathbb{C})_0(\chi)^\vee = L^d_{\alpha,n}(\chi)^\vee$$

is bijection, and the image is spanned by two column vectors

$$\begin{pmatrix}G(\alpha)\\ G'(\alpha)\end{pmatrix}, \quad \begin{pmatrix}G(1-\alpha)\\ G('1-\alpha)\end{pmatrix}$$

with respect to the dual basis of ω_1, ω_2. Note that the action of $\pi_1(S,\alpha)$ on $L^d_{\alpha,n}(\chi)^\vee$ is compatible with that on $H_2(U_{\alpha,n},\mathbb{C})$. Therefore we have an isomorphism

$$L^d_{\alpha,n}(\chi)^\vee \cong \langle G(\alpha), G(1-\alpha)\rangle$$

of $\mathbb{C}[\pi_1(S,\alpha)]$-modules. The right hand side is isomorphic to $V_\alpha = \langle {}_2F_1(\alpha), {}_2F_1(1-\alpha)\rangle$ as $\mathbb{C}[\pi_1(S,\alpha)]$-module, so we are done. □

Let us put $D := x\frac{d}{dx}$ and consider the following differential equation, so-called the hypergeometric equation:

$$\left(D(D-\frac{1}{d}) - x(D+\lambda_1-\frac{1}{d})(D+\lambda_2-\frac{1}{d})\right)u(x) = 0. \tag{3.3.2}$$

Recall that the vector space V_α is the two dimensional vector space over $\mathbb{C}$ spanned by ${}_2F_1(\alpha)$ and ${}_2F_1(1-\alpha)$ where ${}_2F_1(x) = {}_2F_1\left(\begin{smallmatrix}\lambda_1-\frac{1}{d},\lambda_2-\frac{1}{d}\\ 1-\frac{1}{d}\end{smallmatrix}; x\right)$ is the Gaussian hypergeometric function. Then V_α is the space of local solutions of the differential equation (3.3.2). Put

$$H^d_{\lambda_1,\lambda_2} := \mathrm{Im}\big(\pi^1(S,\alpha) \to \mathrm{Aut}(V_\alpha)\big).$$

Lemma 3.3.1 says that

$$H^d_{\lambda_1,\lambda_2} \cong \mathrm{Im}\big(\pi_1(S,\alpha) \to \mathrm{Aut}(L^d_{\alpha,n}(\chi))\big).$$

Therefore, the following proposition finishes the proof of Proposition 3.2.5.

Proposition 3.3.2. *For $d > d_{min}$, $H^d_{\lambda_1,\lambda_2}$ is an infinite group.*

Proof. For $d > d_{min}$, from the Table 3.3, we have

$$0 < \lambda_1 - \frac{1}{d} < \lambda_2 - \frac{1}{d} < 1 - \frac{1}{d} < 1.$$

According to Theorem 4.8 in [7], this inequality implies the infiniteness of the group $H^d_{\lambda_1,\lambda_2}$. □

Chapter 4

Main Results of the Second Work

This chapter is based on [2]. We present a new algorithms to integer factorization. This is developed by combining ECM [16] with CM method [4].

4.1 Preliminaries for the Second Work

In this section, we revisit the basic theory of elliptic curve and summarize its properties which are necessary for describing the second work. In this section, we assume that the characteristic of a field K is neither 2 nor 3.

We introduce some definitions. Let E_1 and E_2 be elliptic curves. An isogeny between E_1 and E_2 is a group homomorphism between $E_1(\overline{K})$ and $E_2(\overline{K})$ which is given by rational functions, i.e. an isogeny $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ can be described by

$$\alpha(x, y) = \Big(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)}\Big)$$

where f_i and g_i $(i = 1, 2)$ are in $\overline{K}[X, Y]$. In the case $E_1 = E_2$, an isogeny is called an endomorphism. We denote the ring of endomorphisms of E by $\mathrm{End}_K(E)$. For $n \in \mathbb{Z}$, the map$[n] : E(\overline{K}) \to E(\overline{K}); P \mapsto nP$ gives the endomorphism of E, that is, can be described by rational functions. We give formulas for these functions later. Then this induces the natural injection $\mathbb{Z} \hookrightarrow \mathrm{End}(E); n \mapsto [n]$. Let E be an elliptic curve over $\mathbb{C}$. It is known that

$\mathrm{End}_{\mathbb{C}}(E)$ is either $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. We say that $E/\mathbb{C}$ has complex multiplication by an order $\mathcal{O}$ if $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}$.

We now describe the map on an elliptic curve E given by multiplication by an integer: for $n \in \mathbb{Z}$, $E(\overline{K}) \to E(\overline{K})$; $P \mapsto nP$. For an elliptic curve $y^2 = x^3 + Ax + B$, we define the division polynomials by

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2Y \\
\psi_3 &= 3X^4 + 6AX^2 + 12BX - A^2 \\
\psi_4 &= 4Y(X^6 + 5AX^4 + 20BX^3 \\
&\quad -5A^2X^2 - 4ABX - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \ (m \geq 2) \\
\psi_{2m} &= \frac{\psi_m}{2Y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \ (m \geq 3)
\end{aligned}$$

and polynomials by

$$\begin{aligned}
\phi_m &= X\psi_m^2 - \psi_{m+1}\psi_{m-1} \\
\omega_m &= \frac{1}{4Y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

Using the division polynomials, we can give the formula for the endomorphism of E given by multiplication by an integer. Let $P = (x, y) \in E(\overline{K})$ be a rational point on E and $n \in \mathbb{Z}$ be a positive integer. Then we have

$$nP = \Big(\frac{\phi_n(x,y)}{\psi_n(x,y)^2}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3}\Big). \tag{4.1.1}$$

Moreover, the following holds:

$$nP = O \Leftrightarrow \psi_n(x, y) = 0. \tag{4.1.2}$$

For an elliptic curve over a field K defined by the equation $y^2 = x^3 + ax + b$ (Proposition 1.1.2), we define the j-invariant of E as follows:

$$j_E := 1728\frac{4a^3}{4a^3 + 27b^2} \in K.$$

Conversely, for given $j_0 \in K$ with $j_0 \neq 0, 1728$, the elliptic curve E defined by the following equation

$$E : y^2 = x^3 + \frac{3j_0}{1728 - j_0}x + \frac{2j_0}{1728 - j_0} \tag{4.1.3}$$

satisfies $j_E = j_0$.

Assumption 4.1.1. In this chapter, we treat elliptic curves E with $j_E \neq 0, 1728$. The excluded case $j_E = 0, 1728$ correspond to the elliptic curves with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-1})$ whose discriminants $-D$ are -3 and -4 respectively. For these cases, see [25] since their class polynomials are of degree 1.

For elliptic curves E_1/K and E_2/K, they are isomorphic over the algebraic closure $\overline{K}$ of K if and only if their j-invariants coincide. This property implies that isomorphic classes of elliptic curves over $\mathbb{C}$ are classified completely by j-invariants. If we work on an arbitrary field K, the condition "isomorphic over K" yields the condition "same j-invariant". However, the converse does not hold. For an elliptic curve E/K, elliptic curves with j-invariant j_E are called twist of E. We identify two twists if they are isomorphic over K.

Proposition 4.1.2. *Let E be an elliptic curve over a finite field $\mathbb{F}_p$ defined by the equation $y^2 = x^3 + ax + b$ with $j_E \neq 0,\ 1728$ (recall the Assumption 4.1.1). Then $\#\{$twists of $E\}/\sim = 2$, where $\sim$ denotes the equivalence relation meaning isomorphic over $\mathbb{F}_p$. Let $c \in \mathbb{F}_p^\times$ be a quadratic nonresidue. Then*

$$E' : y^2 = x^3 + c^2Ax + c^3B$$

is a twist of E which is not isomorphic over $\mathbb{F}_p$.

Proof. See [28], Ch.X, Proposition 5.4. □

4.2 The Elliptic Curve Method

In this section, we give a quick review of Lenstra's algorithm to integer factoring using elliptic curves: the Elliptic Curve Method (ECM). For detail, we refer to [16].

We start with a composite number N that we want to factor. ECM is a method which finds a prime factor of N in the following procedure.

1. Choose several random pairs $(a_i, u_i, v_i) \in \mathbb{Z}/N\mathbb{Z}^{\times 3}$ and define $b_i = v_i^2 - u_i^3 - a_i u_i \in \mathbb{Z}/N\mathbb{Z}$
2. Define elliptic curves $E_i : y^2 = x^3 + a_i x + b_i$, then $P_i = (u_i, v_i) \in E_i(\mathbb{Z}/N\mathbb{Z})$
3. Choose an integer C and compute $(C!)P_i$ on $E_i(\mathbb{Z}/N\mathbb{Z})$
4. If this computation fails for some i, $\gcd(\psi_{C!}(u_i, v_i), N)$ returns a non-trivial divisor of N. If not, start over with a new choice of a family of elliptic curves or an integer C.

Strong points of this method are that we have a rational point of elliptic curves and the process of leading a prime factor of N is trivial. On the other hand, there is a drawback that the generated elliptic curves do not necessarily have a smooth order. Moreover, it is difficult to choose an appropriate bound C.

Our method resolves these drawbacks instead of losing the advantages. Namely, we generate first an elliptic curve with "good" order and find a rational point later. We utilize the CM method for a generation of such an elliptic curve.

4.3 The Complex Multiplication Method

In this section, we recall the complex multiplication method (CM method), which is an algorithm to generate an elliptic curve having a certain order. We note that this method was first used in context of a primality proving [4].

First of all, we recall the definition of the class polynomials of discriminants and the relationship between primes p of special form with respect to a discriminant $-D$ and the class polynomial of $-D$ modulo p. After that, we explain the CM method. For details, see [4], [10], [29] and so forth.

We denote $\mathcal{ELL}(-D)$ by the set of isomorphism classes of elliptic curves over $\mathbb{C}$ with complex multiplication by the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{-D})$:

$$\mathcal{ELL}(-D) := \left\{ [E/\mathbb{C}] \mid \mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}_K \right\}$$

where the notation $[\cdot]$ means an isomorphism class. We can construct an action of $cl(\mathcal{O}_K)$ on $\mathcal{ELL}(-D)$, where $cl(\mathcal{O}_K)$ denotes the ideal class group of

$\mathcal{O}_K$ which is one of the important objects in algebraic number theory, see [10] for example. The order of the group $cl(\mathcal{O}_K)$ is called the class number of $\mathcal{O}_K$. One of the fundamental theorems in algebraic number theory states that the class number of a ring of integers is finite. On the other hand, the fact that this action is simply transitive yields that the class number of $\mathcal{O}_K$ coincides with the order of the set $\mathcal{ELL}(-D)$: $\#cl(\mathcal{O}_K) = \#\mathcal{ELL}(-D)$. Therefore, the set $\#\mathcal{ELL}(-D)$ is a finite set. For details, see [29], Ch.II, §1 .

If we write

$$\mathcal{ELL}(-D) := \Big\{[E_1],\ [E_2],\ \cdots,\ [E_h]\Big\},$$

in virtue of the finiteness, the complex numbers $j_i \in \mathbb{C}$ $(i = 1,\ 2,\ \cdots, h)$ which are distinct from each others are obtained by taking j-invariants of $[E_i]$. We note that, for elliptic curves, the condition "isomorphic over $\mathbb{C}$" is equivalent to the condition "have same j-invariant". Then we define the class polynomial of the discriminant $-D$ as:

$$H_{-D}(T) := \prod_{i=1}^{h}(T - j_i).$$

The class polynomials have integer coefficients, that is, $H_{-D}(T) \in \mathbb{Z}[T]$. The relationship between the class polynomial of a discriminant $-D$ and the quadratic equation $4p = X^2 + DY^2$ for a prime p is stated as the following (see Theorem 3.2 in [4]).

Proposition 4.3.1. *For a discriminant $-D$ and a prime number p, the followings are equivalent:*

1 *The equation $4p = X^2 + DY^2$ has the solution in $\mathbb{Z}$.*

2 *$H_{-D,p}(T)$ splits completely in $\mathbb{F}_p$.*

Here, $H_{-D,p}(T)$ is the image of $H_{-D}(T)$ under the natural morphism $\mathbb{Z}[T] \to \mathbb{F}_p[T]$.

The class polynomials play a key role in the CM method. Our idea is to apply the procedure of ECM to an elliptic curve having "good" order. Here, we utilize the CM method to generate such an elliptic curve. The CM method is a way to construct an elliptic curve $E/\mathbb{F}_p$ with a specified number of $\mathbb{F}_p$-rational points. To be precise, we suppose that a prime number p has a special

form $4p = t^2 + Dv^2$ for some discriminant $-D$ ($D > 4$) and integers $t, v \in \mathbb{Z}$. The integers t^2 and v^2 are uniquely determined by p and $-D$ for $D > 4$. The CM method is a method which generates an elliptic curve $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1 \pm t$ for the above p and t.

Under this assumption, since the class polynomial $H_{-D,p}(T)$ splits completely in $\mathbb{F}_p$, we can take a root $j_0 \in \mathbb{F}_p$ of $H_{-D,p}(T)$. Then we construct an elliptic curve $E_{j_0}/\mathbb{F}_p$ with j-invariant j_0 as in (4.1.3) and write $\#E_{j_0}(\mathbb{F}_p) = p + 1 - a$ ($|a| \leq 2\sqrt{p}$) by Hasse's theorem (see [35],Theorem 4.2 for example). Then, the following holds.

Proposition 4.3.2 ([4],§4.2)**.** *In the above setting, we have the equality $a = \pm t$. Thus if we let E'_{j_0} be a twist of E_{j_0} which is not isomorphic to E_{j_0} over $\mathbb{F}_p$, either E_{j_0} or E'_{j_0} have the order $p + 1 - t$.*

Proof. We use the notation as above. Let $K = \mathbb{Q}(\sqrt{-D})$. For E_{j_0}, there exists an elliptic curve $\widetilde{E}/\mathbb{C}$ with complex multiplication by the ring of integers of K, i.e. $[\widetilde{E}] \in \mathcal{ELL}(-D)$, such that:

$$\mathrm{End}_{\overline{\mathbb{F}}_p}(E_{j_0}) \cong \mathrm{End}_{\mathbb{C}}(\widetilde{E}) \cong \mathcal{O}_K.$$

Elliptic curves over $\mathbb{F}_p$ are endowed with the Frobenius map, which is an endomorphism defined by $(x, y) \mapsto (x^p, y^p)$. The Frobenius map satisfies the quadratic equation $Fr_p^2 - aFr_p + p = 0$ in $\mathrm{End}(E_{j_0})$. Then, via the above isomorphisms, the Frobenius map $Fr_p \in \mathrm{End}_{\overline{\mathbb{F}}_p}(E_{j_0})$ corresponds to a root of the quadratic equation $T^2 - aT + p$ in $\mathcal{O}_K$. The quadratic formula yields that this is equal to

$$\frac{a \pm \sqrt{a^2 - 4p}}{2}$$

and thus we have $\sqrt{a^2 - 4p} \in \mathcal{O}_K$. Therefore, we have $u\sqrt{-D} = \sqrt{a^2 - 4p}$ for some $u \in \mathbb{Z}$. Since the integers t^2 and v^2 are unique for the representation $4p = t^2 + Dv^2$, we obtain the equalities: $t^2 = a^2$ and $u^2 = v^2$. We are done for the first part of the claim. The second part of the claim follows from Proposition 4.1.2. □

4.4 Setting

Now, we start explaining our proposed algorithm.

Let $-D$ be a discriminant and $N = pq$ be a composite number. Throughout this section, we assume that a prime number p has the form: $4p = t^2 + Dv^2$ for some $t, v \in \mathbb{Z}$. For the class polynomial $H_{-D}(T_1)$, we define a ring:

$$R_N^{-D} := \mathbb{Z}/N\mathbb{Z}[T_1]/\big(H_{-D,N}(T_1)\big).$$

where $H_{-D,N}(T_1)$ is the image of $H_{-D}(T_1)$ under the natural morphism $\mathbb{Z}[T_1] \to \mathbb{Z}/N\mathbb{Z}[T_1]$. For a random element $c \in \mathbb{Z}/N\mathbb{Z}$, put $A^{-D,c}(T_1) := \frac{3c^2T_1}{1728-T_1}$ and $B^{-D,c}(T_1) := \frac{2c^3T_1}{1728-T_1}$, and we define an elliptic curve $E^{-D,c}$ over the ring R_N^{-D} as follows:

$$E^{-D,c} : y^2 = x^3 + A^{-D,c}(T_1)x + B^{-D,c}(T_1). \tag{4.4.1}$$

Then we have $j_{E^{-D,c}} = T_1$.

By the assumption about the form of p, we can take a root j_0 of the class polynomial $H_{-D,p}(T_1)$ in $\mathbb{F}_p$ (see Proposition 4.3.1). By substituting T_1 for j_0 in the equation of $E^{-D,c}$, we obtain the elliptic curve over $\mathbb{F}_p$:

$$E^{-D,c}_{T_1=j_0} : y^2 = x^3 + A_p^{-D,c}(j_0)x + B_p^{-D,c}(j_0)$$

with j-invariant j_0. Then the CM method implies that

$$\#E(\mathbb{F}_p) = p + 1 \pm t.$$

The next thing that we have to do is to find a rational point of $E^{-D,c}$. We will construct a rational point of $E^{-D,c}$ by extending the coefficient ring R_N^{-D}. We choose a random element $x_0 \in \mathbb{Z}/N\mathbb{Z}$ and define a polynomial

$$\tau(T_1) := x_0^3 + A^{-D,c}(T_1)x_0 + B^{-D,c}(T_1). \tag{4.4.2}$$

Set

$$S_N^{-D,\tau(T_1)} := R_N^{-D}[T_2]/\big(T_2^2 - \tau(T_1)\big).$$

Then we obtain a rational point naturally:

$$P := (x_0, T_2) \in E^{-D,c}\big(S_N^{-D,\tau(T_1)}\big).$$

Using the formula (4.1.1), we can write

$$nP = \Big(\frac{\phi_n(x_0,T_2)}{\psi_n^2(x_0,T_2)}, \frac{\omega_n(x_0,T_2)}{\psi_n^3(x_0,T_2)}\Big) \in E^{-D,c}(S_N^{-D,\tau(T_1)})$$

and in $S_N^{-D,\tau(T_1)}$

$$\psi_n(x_0, T_2) = g_{n,0}(T_1) + g_{n,1}(T_1)T_2,$$

where $g_{n,i}(T_1) \in \mathbb{Z}/N\mathbb{Z}[T_1]$ with $\deg\big(g_{n,i}(T_1)\big) < \deg\big(H_{-D}(T_1)\big)$ $(i = 0, 1)$.

4.5 Our Proposed Algorithms

In the above setting, we state the key fact for the algorithms.

Theorem 4.5.1. *Notation as above. Suppose that $t = 1$. Moreover, we assume that $\#E(\mathbb{F}_p) = p$ and $\tau_p(j_0) \in \mathbb{F}_p$ is a quadratic residue. Then, we have*

$$\gcd\big(\mathrm{Res}(H_{-D,N}(T), g_{N,0}^2(T) - g_{N,1}^2(T)\tau(T)), N\big) \neq 1.$$

Here, $\mathrm{Res}(\cdot,\cdot)$ *denotes the resultant.*

Proof. By the assumption, there exists $\sigma \in \mathbb{F}_p$ such that $\sigma^2 = \tau_p(j_0)$. Then, the homomorphism

$$S_N^{-D,\tau(T_1)} \to \mathbb{F}_p;\ T_1 \mapsto j_0,\ T_2 \mapsto \sigma$$

induces $E^{-D,c}\big(S_N^{-D,\tau(T_1)}\big) \to E^{-D,c}(\mathbb{F}_p)$. We denote the image of $P \in E^{-D,c}(S_N^{-D,\tau(T_1)})$ under this morphism by $P_p \in E^{-D,c}_{T_1=j_0}(\mathbb{F}_p)$.

Moreover, the assumption $\#E^{-D,c}(\mathbb{F}_p) = p$ yields $NP_p = \infty \in E^{-D,c}_{T_1=j_0}(\mathbb{F}_p)$. Thus, by (4.1.2), we have

$$\psi_N(x_0, \sigma) = g_{N,0}(j_0) + g_{N,1}(j_0)\sigma = 0 \in \mathbb{F}_p$$

and then

$$\tau_p(j_0) = \frac{g_{N,0}(j_0)^2}{g_{N,1}(j_0)^2} \in \mathbb{F}_p.$$

Since j_0 is a root of $H_{-D,p}(T)$ in $\mathbb{F}_p$, this means that two polynomials $H_{-D,p}(T)$ and $g_{N,0}(T)^2 - g_{N,1}(T)^2\tau(T)$ have a common root in $\mathbb{F}_p$. Therefore, we have

$$\gcd\big(\mathrm{Res}(H_{-D,N}(T), g_{N,0}^2(T) - g_{N,1}^2(T)\tau(T)), N), N\big) \equiv 0 \bmod p,$$

so we are done. □

This theorem leads Algorithm 1. On the other hand, the following theorem leads Algorithm 2.

Theorem 4.5.2. *Notation as above. Suppose that $p + 1 - t$ is C-smooth, i.e. $p + 1 - t \mid C!$. Put $M = C!$. Moreover, we assume that $\#E(\mathbb{F}_p) = p + 1 - t$ and $\tau_p(j_0) \in \mathbb{F}_p$ is a quadratic residue. Then, we have*

$$\gcd\big(\mathrm{Res}(H_{-D,M}(T), g_{M,0}^2(T) - g_{M,1}^2(T)\tau(T)), N\big) \neq 1.$$

Proof. The same discussion as above is valid if we add slight modifications. □

The above discussion leads to the algorithms in the next page.

Algorithm 1

Input : a composite integer N
a discriminant $-D$, the class polynomial $H_{-D}(T)$ of $-D$

Output : a prime factor of N

1. Choose a random element $c \in \mathbb{Z}/N\mathbb{Z}$
2. Define an elliptic curve over R_N^{-D} by the equation (4.4.1)
3. Choose a random element $x_0 \in \mathbb{Z}/N\mathbb{Z}$ and define $\tau(T_1)$ as (4.4.2)
4. Take the rational point $P = (x_0, T_2) \in E^{-D,c}(S_N^{-D,\tau(T_1)})$
5. Compute NP
6. Compute $\gcd\big(\mathrm{Res}(H_{-D,N}(T), g_{N,0}^2(T) - g_{N,1}^2(T)\tau(T)), N\big)$

6-1. If it is non-trivial divisor of N, we are done.

6-2. If not, start over with a new choice of $c \in \mathbb{Z}/N\mathbb{Z}$ or $x_0 \in \mathbb{Z}/N\mathbb{Z}$

Algorithm 2

Input : a composite integer N, $M = C!$ for a bound C
a discriminant $-D$, the class polynomial $H_{-D}(T)$ of $-D$

Output : a prime factor of N

1. Choose a random element $c \in \mathbb{Z}/N\mathbb{Z}$
2. Define an elliptic curve by the equation (4.4.1)
3. Choose a random element $x_0 \in \mathbb{Z}/N\mathbb{Z}$ and define $\tau(T_1)$ as (4.4.2)
4. Take the rational point $P = (x_0, T_2) \in E^{-D,c}(S_N^{-D,\tau(T_1)})$
5. Compute MP
6. Compute $\gcd\big(\mathrm{Res}(H_{-D,M}(T), g_{M,0}^2(T) - g_{M,1}^2(T)\tau(T)), N\big)$

6-1.If it is non-trivial divisor of N, we are done.

6-2. If not, start over with a new choice of $c \in \mathbb{Z}/N\mathbb{Z}$ or $x_0 \in \mathbb{Z}/N\mathbb{Z}$

We discuss the success conditions and success probabilities for our proposed algorithms. Algorithm 1 fails when $t \neq \pm 1$, and Algorithm 2 fails when $p+1 \pm t$ is not a divisor of $C!$. Also when $t = \pm 1$ in Algorithm 1 or when $p+1 \pm t$ is a divisor of $C!$ in Algorithm 2, these may fail depending on how to select $c \in \mathbb{Z}/N\mathbb{Z}$ or $x_0 \in \mathbb{Z}/N\mathbb{Z}$, but its probability is not so high. So, if one selects c or x_0 sufficiently many times, the algorithms succeed with high probability. Conversely, if these do not succeed, it is highly probable that the above conditions for t are not satisfied.

In detail, if c is chosen at random, it is expected that the order of $E(\mathbb{F}_p)$ will be randomly determined from two ways $p+1 \pm t$, one of which is appropriate and the other is inappropriate. So, there is a possibility that the algorithm fails with a probability of $\frac{1}{2}$ with respect to how to select c. Therefore, the expected value of the number of times to choose c before the algorithm succeeds is considered to 2.

Also, if x_0 (and c) is chosen at random, for each of the roots $j_1, \ldots, j_h$ of $H_{-D}(T)$, the probability that $\tau_p(j_i)$ is not a quadratic residue is expected to be $\frac{1}{2}$. The algorithms fail when this happens for all j_i. So, assuming that the behaviors whether $\tau_p(j_i)$ is a quadratic residue are independent of each other, the probability that this causes a failure of the algorithms is thought to be $(\frac{1}{2})^h$. Therefore, for each c, the expected value of the number of times to choose x_0 before the algorithm succeeds is less than or equal to 2, and when h is large this expected value is close to 1.

On the other hand, for solving the equation $4p = X^2 + DY^2$, there is an efficient algorithm given by Cornacchia[9], which is easy to describe, see [6] or [8] §1.5.2. As our proposed algorithm with input discriminant $-D$ is effective only when a prime factor p of N satisfies $4p = X^2 + DY^2$ for some X, Y, the attack by our algorithm will be avoidable by, for example, checking (in the key generation phase) whether or not the equation $4p = X^2 + DY^2$ has a solution and then by discarding the prime p if a solution exists.

Here, we describe the process of our proposed algorithm in step by step by using a small example. We give a toy example of Algorithm 2 only, since the structure of Algorithm 1 is almost the same as Algorithm 2.

Example 4.5.3. We attempt to factor $N = 793 = 61 \cdot 13$ using Algorithm 2 with $C = 5$. Since $4 \cdot 61 = 2^2 + 15 \cdot 4^2$ and $61 + 1 - 2 = 60$ is a divisor of $C! = 120$, if we choose the discriminant $-D = -15$, Algorithm 2 should be successful.

Firstly we choose $c = 1$ in $\mathbb{Z}/793\mathbb{Z}$ and construct an elliptic curve $E^{-15,1}$ over the ring $R_{793}^{-15} = \mathbb{Z}/793\mathbb{Z}[T_1]/(H_{-15,793}(T_1))$ as (4.4.1) where the class polynomial of -15 is:

$$H_{-15}(T_1) = T_1^2 + 191025T_1 - 121287375 \in \mathbb{Z}[T_1].$$

Since we can write $4 \cdot 61 = 2^2 + 15 \cdot 4^2$, the polynomial $H_{-15,61}(T_1)$ splits completely in $\mathbb{F}_{61}$ as follows:

$$\begin{aligned} H_{-15,61}(T_1) &= T_1^2 + 34T_1 + 23 \\ &= (T_1 + 5)(T_1 + 29) \in \mathbb{F}_{61}[T_1] \end{aligned}$$

So, by the CM method, if we substitute a root $-5 = 56$ of $H_{-15,61}(T_1)$ in $\mathbb{F}_{61}$ for T_1in the coefficients of $E^{-15,1}$, the order of $E^{-15,1}_{T_1=56}(\mathbb{F}_{61})$ should be $61 + 1 \pm 2 = 60$ or 64 since its j-invariant is equal to 56. Indeed, $\#E^{-15,1}_{T_1=56}(\mathbb{F}_{61}) = 60$.

Secondly, we take $x_0 = 4$ and define $\tau(T_1)$ as (4.4.2). Then, $\tau_{61}(56) = 49 \in \mathbb{F}_{61}$ is a quadratic residue in $\mathbb{F}_{61}$. By extending the coefficient ring, we obtain a rational point over the ring $S_{793}^{-15,\tau(T_1)}$:

$$P = (4, T_2) \in E^{-15,1}(S_{793}^{-15,\tau(T_1)}).$$

where $S_{793}^{-15,\tau(T_1)} = \mathbb{Z}/793\mathbb{Z}[T_1, T_2]/(H_{-15,793}(T_1), T_2 - \tau(T_1))$.

Finally, Algorithm 2 should succeed since $\#E^{-15,1}_{T_1=56}(\mathbb{F}_{61}) = 60$ is 5-smooth. Indeed, we compute the division polynomial $\psi_{5!}$ by using the recurrence relation in §2.2,

$$\begin{aligned} \psi_{5!}(4, T_2) &= g_{5!,0}(T_1) + g_{5!,1}(T_1)T_2 \\ &= (549T_1 + 61)T_2 \in S_{793}^{-15,\tau(T_1)} \end{aligned}$$

and we compute

$$g_{5!,0}^2(T_1) - g_{5!,1}^2(T_1)\tau(T_1) = 488T_1 + 488 \in \mathbb{Z}/793\mathbb{Z}[T_1].$$

So, we obtain

$$\mathrm{Res}(H_{-15,793}(T_1), 488T_1 + 488) = 61.$$

Therefore, the computation of the step 6 in Algorithm 2 outputs

$$\begin{aligned}\gcd(\mathrm{Res}(H_{-15,793}(T_1), 488T_1 + 488), 793) &= \gcd(61, 793)\\ &= 61.\end{aligned}$$

Algorithm 2 succeeds since 61 is a divisor of 793.

Example 4.5.4. Here we show some examples of discriminants $-D$ and prime factors p for which our generalized algorithm can factorize the integer $N = pq$ while the previous algorithm in [25] is not effective.

1. $N = p \times q = 5044150429022801115530654941193$
   $p = 57094208850412$
   $q = 883478470161233$
   $-D = -23$ $(\deg H_{-D}(X) = 3)$
   $4p = t^2 + D \times 9961456^2$ $(t = 1210134)$
   $p + 1 - t = 570942087293988 \mid 2000!$

2. $N = p \times q = 488391904291$
   $p = 804161$
   $q = 607331$
   $-D = -56$ $(\deg H_{-D}(X) = 4)$
   $4p = t^2 + D \times 232^2$ $(t = 450)$
   $p + 1 - t = 803712 = 2^7 \times 3 \times 7 \times 13 \times 23$

3. $N = p \times q = 55054741897698566681622677988503082855882698696757826795561 1$
   $p = 6338253001150313676073094416 63$
   $q = 8686106706012969085624341961 97$
   $-D = -131$ $(\deg H_{-D}(X) = 5)$
   $4p = 1 + D \times 139116657084339^2$

Bibliography

[1] Y. Aikawa, *The Bounds of Mordell-Weil Ranks in Cyclotomic Towers of Function Fields*, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.01.003.

[2] Y. Aikawa, K. Nuida, M. Shirase, *Elliptic Curve Method using Complex Multiplication Method*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E102-A, no.1 (2019) 74–80 .

[3] M. Asakura and N. Otsubo, *Regulators of K_1 for Hypergeometric fibrations*, To appear in the Proceedings of Conference "Arithmetic L-functions and Differential Geometric Methods (Regulators IV)", arXiv:1709.04144.

[4] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving.* Math. Comp. 61 (1993), no. 203, 29-68.

[5] W. Barth, K. Hulek,C. Peters, and A. Van de Ven, *Compact Complex Surfaces*, second edition, Springer-Verlag, Berlin, 2004.

[6] J. M. Basilla, *On the solution of $x^2 + dy^2 = m$.* Proc. Japan Acad. Ser. A Math. Sci. 80 (2004), no. 5, 40-41.

[7] F. Beukers, G. Heckman, *Monodromy for the hypergeometric function ${}_nF_{n-1}$*, Invent. Math. 95 (1989), no. 2, 325-354.

[8] H. Cohen, *A course in computational algebraic number theory.* Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[9] G. Cornacchia, *Su di un metodo per la risoluzione in numeri interi dell' equazione* $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$. Giornale di Mat. di Battaglini 46 (1908), 33-90.

[10] D. A. Cox, *Primes of the Form* $x^2 + ny^2$*, Second edition.* John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[11] J. S. Ellenberg, *Selmer groups and Mordell-Weil groups of elliptic curves over towers of function fields*, Compos. Math. 142 (2006), no. 5, 1215-1230.

[12] L. A. Fastenberg, *Mordell-Weil groups in procyclic extensions of a function field*, Duke Math. J. 89 (1997), no.2, 217-224.

[13] L. A. Fastenberg, *Computing Mordell-Weil ranks of cyclic covers of elliptic surfaces*, Proc. Amer. Math. Soc. 129 (2001), no. 7, 1877-1883.

[14] Schmickler-Hirzebruch. U, *Elliptische Flächen über* $P_1\mathbb{C}$ *mit drei Ausnahmefasern und die hypergeometrische Differentialgleichung.* Schriftenreihe des Mathematischen Instituts der Universität Münster, 2. Serie , 33. Universität Münster, Mathematisches Institut, Münster, 1985. 170 pp.

[15] K.Kodaira, *On compact complex analytic surface I*, Ann.Math.71(1960), 111-152. *II*, Ann.Math.77(1963), 563-626. *III*, Ann.Math.78(1963), 1-40.

[16] H. W. Lenstra, Jr., *Factoring integers with elliptic curves.* Ann. of Math. (2) 126 (1987), no. 3, 649-673.

[17] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math.18 (1972), 183-266.

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

[19] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), no.2, 129-162.

[20] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Philos. Soc. 21 (1922), 179-192.

[21] A. Pál , *Hodge Theory and the Mordell-Weil rank of elliptic curves over extensions of function fields*, J. Number Theory 137 (2014), 166-178.

[22] M. Schütt, T. Shioda, *Elliptic Surfaces*, Algebraic geometry in East Asia-Seoul 2008, 51-160, Adv. Stud. Pure Math., 60, Math. Soc. Japan, Tokyo, 2010.

[23] T. Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. 108 (1986), no. 2, 415-432.

[24] T. Shioda, *On the Mordell-Weil lattices*, Comment.Math.Univ.St.Paul.39(1990), no.2, 211-240.

[25] M. Shirase, *Condition on composite numbers easily factored with elliptic curve method*, IACR Cryptology ePrint Archive, 2017/403. `https://eprint.iacr.org/2017/403`.

[26] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer, New York,1994.

[27] J. H. Silverman, *A bound for the Mordell-Weil rank of an elliptic surface after a cyclic base extension*, J. Algebraic Geom. 9 (2000), no. 2, 301-308.

[28] J. H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition.* Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[29] J. H. Silverman, *The Rank of Elliptic Surfaces in Unramified Abelian Towers*, J. Reine Angew. Math. 577 (2004), 153-169.

[30] P. Stiller, *The Picard Number of Elliptic Surfaces with Many Symmetries*, Pacific J.Math.128(1987), no.1, 157-189.

[31] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variables IV, Lect. Note in Math. 467, B. J. Birch and W. Kuyk, eds., Springer-Verlag, Berlin, 1975, 33-52.

[32] D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math.(2)155(2002), no.1, 295-315.

[33] D. Ulmer, *Elliptic curves and analogies between number fields and function fields*, In Heegner Points and Rankin L-Series (Mathematical Sciences Research Institute Publications, 285-316). Cambridge University Press, Cambridge, 2004.

[34] C. Voisin, *Hodge theory and complex algebraic geometry. I*, Cambridge Studies inAdvanced Mathematics, 76., Cambridge University Press, Cambridge, 2002.

[35] L. C. Washington, *Elliptic curves. Number Theory and Cryuptography. Second Edition.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2008.

[36] A, Weil, *L'arismètique sur les courbes algébriques.* Acta Math. 52 (1929), no. 1, 281-315.