On two problems about isogenies of elliptic curves over finite fields

Lixia Luo[a,b], Guanju Xiao[a,b], Yingpu Deng[a,b]

[a]*Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, People's Republic of China*
[b]*School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, People's Republic of China*

Abstract

Isogenies occur throughout the theory of elliptic curves. Recently, the cryptographic protocols based on isogenies are considered as candidates of quantum-resistant cryptographic protocols. Given two elliptic curves E_1, E_2 defined over a finite field k with the same trace, there is a nonconstant isogeny β from E_2 to E_1 defined over k. This study gives out the index of $\text{Hom}_k(E_1, E_2)\beta$ as a left ideal in $\text{End}_k(E_2)$ and figures out the correspondence between isogenies and kernel ideals. In addition, some results about the non-trivial minimal degree of isogenies between the two elliptic curves are also provided.

Keywords: Elliptic curve, Isogeny, Kernel ideal, Minimal degree.

1. Introduction

Isogenies play an important part in the theory of elliptic curves. A recent research area is cryptographic protocols based on the difficulty of constructing isogenies between elliptic curves over finite fields[2, 5, 8]. These cryptographic protocols are supposed to resist the quantum computations. To get more facts about isogenies, this paper concerns two problems related to isogenies.

Let F be a perfect field, and E_1, E_2 be elliptic curves defined over F, it had been proved that $\text{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank at most 4 [14, Corollary III.7.5]. Further, the possible ranks of $\text{End}(E_1)$ (or $\text{End}(E_2)$) are $1, 2, 4$. The possible result that $\text{rank}_{\mathbb{Z}} \text{Hom}(E_1, E_2) = 3$ is proved to be negative. If there is a nonconstant isogeny β from E_2 to E_1, $\text{Hom}(E_1, E_2)\beta$ is a left ideal of $\text{End}(E_2)$, then $\text{rank}_{\mathbb{Z}}\text{Hom}(E_1, E_2) = \text{rank}_{\mathbb{Z}}\text{End}(E_2)$. The index of $\text{Hom}(E_1, E_2)\beta$ in $\text{End}(E_2)$ is finite, but the exact result needs to be identified. We assume that the characteristic of F is not 0 and for the cases $\text{char}(F) = 0$, we discuss them in Appendix A.

In Waterhouse's thesis[21], he introduced the concept of kernel ideals and proved that for any elliptic curve E over a finite field, the left ideals of its endomorphism ring are all kernel ideals. Every such left ideal can induce an isogeny from E, and ideal multiplication corresponds to isogeny composition. Kohel proved the correspondence between the invertible ideals and the isogenies between two ordinary elliptic curves with the same endomorphism type and used the invertible ideals of imaginary quadratic orders to compute the endomorphism types of ordinary elliptic curves over finite fields[9]. In this paper, we explore the index of $\text{Hom}_k(E_1, E_2)\beta$ as a left ideal in $\text{End}_k(E_2)$ for any nonconstant isogeny β from E_2 to E_1 defined over a finite field k as the first problem. For ordinary elliptic curves, not all isogenies can correspond to kernel ideals. We will give out a way to judge whether the isogenies correspond to kernel ideals in this case. Besides, it is natural for us to consider the non-trivial minimal degree of isogenies between any two elliptic curves over finite fields as the second problem.

The paper is organized as follows. In Section 2, we provide the preliminaries on elliptic curves, isogenies, endomorphism rings and kernel ideals. The answer to the first problem will be given

out by Theorems 3.1 and 3.2 in Section 3. And the study of the second problem can be found in Section 4.

2. Preliminaries

2.1. Elliptic curves and isogenies

Let k be a finite field of characteristic p and let E be an elliptic curve defined over k. E can be written in a generalised Weierstrass equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

For simplicity, if $p > 3$, up to k-isomorphism, E can be written as the short Weierstrass form

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

with its discriminant $4A^3 + 27B^2$ not equal to 0. Under this form the j-invariant of E is defined as $1728(4A^3)/(4A^3 + 27B^2)$, which is an invariant up to $\bar{k}$-isomorphism. $E(k)$ is a finite abelian group with unity ∞ under the chord and tangent addition law [20].

Let E_1 and E_2 be two elliptic curves defined over k. An isogeny α from E_1 to E_2 is a morphism mapping ∞ to ∞. If $\alpha(E_1) = \infty$, α is called constant and denoted by 0. Its degree is defined to be 0. Otherwise, α can be represented as $(r_1(x), r_2(x)y)$ where $r_1(x)$, $r_2(x)$ are rational functions and we can write $r_1(x) = p(x)/q(x)$ with polynomials $p(x)$ and $q(x)$ that don't have a common factor and $q(x) \neq 0$. The degree of α is defined to be

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}.$$

α is called separable if $(r_1(x))' \neq 0$. All nonconstant isogenies are surjective homomorphisms with finite kernels and $|\ker(\alpha)| = \deg \alpha$ if α is separable [20]. According to [14, Proposition III.4.12], the nonconstant separable isogenies from a given elliptic curve can be distinguished by their kernels. For every nonconstant isogeny $\beta : E_2 \to E_1$ of degree m, there is a unique dual isogeny $\widehat{\beta} : E_1 \to E_2$ satisfying $\widehat{\beta}\beta = [m]_{E_2}$ and $\beta\widehat{\beta} = [m]_{E_1}$ where $[m]$ is the multiplication-by-m map of degree m^2 and $\deg \widehat{\beta} = m$ [14, Theorem III.6.1]. For the properties of dual isogenies, we can refer to [14, Theorem III.6.2]. All the isogenies we consider in the following are nonconstant.

Let $\mathrm{Hom}(E_1, E_2)$ denote the collection of all isogenies from E_1 to E_2. Similarly, $\mathrm{Hom}_k(E_1, E_2)$ can be defined for the isogenies defined over k. If $E_1 = E_2$, the isogenies are called endomorphisms. All endomorphisms of an elliptic curve E form a ring and it is called the endomorphism ring of E and denoted by $\mathrm{End}(E)$. The endomorphism ring defined over k is denoted by $\mathrm{End}_k(E)$.

Let $q = |k|$ and $t = q + 1 - |E(k)|$. Then the Frobenius endomorphism $\phi_{q,E} : (x, y) \mapsto (x^q, y^q)$ of E related to k has characteristic polynomial $h_{q,E} := x^2 - tx + q$. t is called the trace of $\phi_{q,E}$ or E over k. By Hasse's theorem, we have $t^2 - 4q \leqslant 0$. Let $\pi_{q,E}$ be a root of $h_{q,E}$. If there is a nonconstant isogeny from E_1 to E_2 defined over k, E_1 and E_2 are called k-isogenous. It is well known that E_1 and E_2 are k-isogenous if and only if $h_{q,E_1} = h_{q,E_2}$ if and only if $|E_1(k)| = |E_2(k)|$ [18, Theorem 1]. All the k-isogenous elliptic curves form an isogeny class over k.

2.2. Endomorphism rings and kernel ideals

An elliptic curves E is called supersingular if $p \mid t$ and ordinary, otherwise. As we all know, $\mathrm{End}(E)$ is isomorphic to an imaginary quadratic order containing $\pi_{q,E}$ when E is ordinary or a maximal order of a definite quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified at p and ∞ when E is supersingular[14, Theorem V.3.1]. According to Waterhouse's thesis[21, Theorem 4.2], $\mathrm{End}_k(E)$ is equal to $\mathrm{End}(E)$ when $p \nmid t$ or $t = \pm 2\sqrt{q}$ and for other cases, $\mathrm{End}_k(E)$ is isomorphic to an imaginary quadratic order which is ramified at p containing $\pi_{q,E}$. Then $\mathrm{End}(E)(\mathrm{End}_k(E)) \otimes \mathbb{Q}$ is isomorphic to an imaginary quadratic field or $B_{p,\infty}$. In general, we will denote the field or the algebra by K, and we call it endomorphism algebra. The isogenous elliptic curves have the same endomorphism algebra.

Any definite quaternion algebra over $\mathbb{Q}$ has a representation of the form $\left(\frac{a,b}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ where $i^2 = a, j^2 = b, k = ij = -ji$. Define the conjugation of the elements of $\left(\frac{a,b}{\mathbb{Q}}\right)$ given by

$$\alpha = x + yi + zj + wk \mapsto \bar{\alpha} = x - yi - zj - wk,$$

2

from which the reduced trace and norm take the form

$$\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2x \text{ and } \mathrm{Nrd}(\alpha) = \alpha\bar{\alpha} = x^2 - ay^2 - bz^2 + abw^2.$$

For simplicity, we use the same symbols for the trace and norm of imaginary quadratic fields. Let $i_E : K \to \mathrm{End}(E) \otimes \mathbb{Q}$ be an isomorphism, then every endomorphism α and its dual satisfy the characteristic polynomial $x^2 - \mathrm{Trd}(i_E^{-1}(\alpha))x + \mathrm{Nrd}(i_E^{-1}(\alpha))$. Under this isomorphism, the dual of every endomorphism corresponds to the conjugate of the corresponding element in the imaginary quadratic field or the conjugation of the corresponding element in $B_{p,\infty}$. And the degree corresponds to the field norm of the imaginary quadratic field or the reduced norm of $B_{p,\infty}$.

Let $\beta : E_2 \to E_1$ be an isogeny defined over k. Let $i_{E_2} : K \to \mathrm{End}_k(E_2) \otimes \mathbb{Q}$ be an isomorphism and fix $i_{E_2}(\pi_{q,E_2}) = \phi_{q,E_2}$, then we can induce

$$i_{E_1} : K \to \mathrm{End}_k(E_1) \otimes \mathbb{Q}$$

$$\zeta \mapsto \frac{1}{\deg(\beta)} \beta i_{E_2}(\zeta)\widehat{\beta}$$

where $\widehat{\beta}$ is the dual isogeny of β and $i_{E_1}^{-1}(\phi_{q,E_1}) = i_{E_2}^{-1}(\phi_{q,E_2})$. Hence under these two isomorphisms, we have

$$i_{E_2}^{-1}(\mathrm{Hom}_k(E_1, E_2)\beta) = i_{E_1}^{-1}(\beta\mathrm{Hom}_k(E_1, E_2)).$$

In the following, for simplicity, we take $\mathrm{End}_k(E)$ as an order of K and take $\mathrm{Hom}_k(E_1, E_2)\beta$ as $i_{E_2}^{-1}(\mathrm{Hom}_k(E_1, E_2)\beta)$, then $\mathrm{Hom}_k(E_1, E_2)\beta = \beta\mathrm{Hom}_k(E_1, E_2))$ is a left ideal of $\mathrm{End}_k(E_2)$ and a right ideal of $\mathrm{End}_k(E_1)$. Since $i_{E_2}^{-1}(\widehat{\alpha})$ is equal to $\overline{i_{E_2}^{-1}(\alpha)}$, then

$$i_{E_1}^{-1}(\mathrm{Hom}_k(E_2, E_1)\widehat{\beta}) = i_{E_2}^{-1}(\widehat{\beta}\mathrm{Hom}_k(E_2, E_1)) = \overline{i_{E_2}^{-1}(\mathrm{Hom}_k(E_1, E_2)\beta)}.$$

We now investigate kernel ideals and their relations with isogenies. The main references are Waterhouse's thesis[21] and [19, Chapter 42.2]. For an isogeny β from an elliptic curve E defined over k, let $\mathrm{H}(\beta)$ be its kernel as a finite group scheme over k. Define the rank of a finite group scheme H as $\dim_k k[H]$. And rank $\mathrm{H}(\beta) = \deg\beta$. Give an non-zero ideal J of $\mathrm{End}_k(E)$, let $\mathrm{H}(J)$ be the scheme-theoretic intersection of the kernels of all elements of J. Let $\mathrm{I}(H) := \{\alpha \in \mathrm{End}_k(E) : \alpha(H) = \infty\}$. J is called kernel ideal if $J = \mathrm{I}(\mathrm{H}(J))$. In fact, all the ideals considered in this paper are kernel ideals due to [21].

Proposition 2.1. *Given an elliptic curve E over finite field k.*

1) *If $\mathrm{End}(E)$ is isomorphic to a maximal order of quaternion algebra, then every ideal I of $\mathrm{End}(E)$ is a kernel ideal, and rank $\mathrm{H}(I)$ is equal to the reduced norm $\mathrm{Nr}(I)$.*

2) *If $\mathrm{End}(E)$ is isomorphic to an imaginary quadratic order, then every ideal I of $\mathrm{End}(E)$ is a kernel ideal, and if I is invertible, then rank $\mathrm{H}(I)$ is equal to the norm of I.*

Proof. See[21, Theorems 3.15 and 4.5]. If $\mathrm{End}(E)$ is not maximal, for every invertible ideal I, it is similar to the proof of Theorem 3.15 where Waterhouse just proved for the case when $\mathrm{End}(E)$ is maximal that rank $\mathrm{H}(I)$ is equal to the norm of I. $\square$

Waterhouse also proved that ideal multiplication corresponds to composition of isogenies.

Proposition 2.2. *Let I be a left ideal of the endomorphism ring $\mathrm{End}_k(E)$, $\varphi_I : E \to E/\mathrm{H}(I) = E'$ be the isogeny with kernel $H(I)$. Let J be a left ideal of $\mathrm{End}_k(E')$, $\varphi_J : E' \to E'/\mathrm{H}(J) = E''$. Then $\varphi_J\varphi_I$ is the isogeny from E to E'' with kernel $H(IJ)$.*

Proof. See[21, Proposition 3.12]. $\square$

If an isogeny from E has kernel $\mathrm{H}(J)$ for some ideal J of $\mathrm{End}_k(E)$ or $\mathrm{End}(E)$, then we say the isogeny are corresponding to J and J is the kernel ideal of the isogeny. In Waterhouse's thesis, he mentioned that not every finite subgroup of E has the form $\mathrm{H}(J)$. In fact, we will give out a way to judge whether the isogenies can correspond to ideals in Section 3.

Let $\beta : E_2 \to E_1$ be an isogeny defined over k. If $\deg(\beta)$ is prime to p, then $H(\beta)=\ker(\beta)$ as a subgroup of $E_2(\bar{k})$ which is closed under the action of the Galois group of $\bar{k}$ over k. Otherwise, we do some discussion following.

Given an elliptic curve E defined over $k = \mathbb{F}_{p^n}$, the Frobenius map $\phi_{p,E} : E \to E^{(p)}$ with $(x,y) \to (x^p, y^p)$ is defined over k. And if $E : y^2 = x^3 + Ax + B$, then $E^{(p)} : y^2 = x^3 + A^p x + B^p$. Although $\ker(\phi_{p,E})=\{\infty\}$, $H(\phi_{p,E})$ is a finite group scheme of rank p and $\mathrm{Hom}(E^{(p)}, E)\phi_{p,E}$ is the kernel ideal of $(\phi_{p,E})$. And $\phi_{p^i,E} : E \to E^{(p^i)}$ with $(x,y) \to (x^{p^i}, y^{p^i})$ is equal to $\phi_{p,E^{(p^{i-1})}} \cdots \phi_{p,E^{(p)}} \phi_{p,E}$ where $i \in \mathbb{Z}_{>0}$ and $\phi_{p^n,E}$ is the Frobenius endomorphism of E over k. If $\beta \in \mathrm{Hom}(E_2, E_1)$ is not separable, by [14, Corollarly II.2.12], β can be factored as

$$E_2 \overset{\phi_{q'}}{\to} E_2^{(q')} \overset{\lambda}{\to} E_1,$$

where $\phi_{q'}$ is the q'th-power Frobenius map, q' is the inseparable degree of β and the map λ is separable.

If E is supersingular, then $\widehat{\phi_{p^n,E}}$ is purely inseparable. Let β be any isogeny from E of degree p^e, then $\beta = \lambda\phi_{p^e,E}$, where λ is an isomorphism. By Proposition 2.2, β corresponds to the following ideal

$$\mathrm{Hom}(E^{(p)}, E)\phi_{p,E}\mathrm{Hom}(E^{(p^2)}, E^{(p)})\phi_{p,E^{(p)}} \cdots \mathrm{Hom}(E^{(p^e)}, E^{(p^{e-1})})\phi_{p,E^{p^{(e-1)}}}.$$

Given a maximal order type containing some order $\mathcal{O}$, whose localization $\mathcal{O}_p$ has unique maximal two-sided ideal $\mathfrak{P}$. According to Deuring's correspondence between supersingular j-invariants and the types of maximal orders in $B_{p,\infty}$[7, Chapter 10.2][9, Theorem 44], if $\mathfrak{P}$ is principal, then there is only one j-invariant which is defined over $\mathbb{F}_p$ such that its endomorphism ring corresponds to this type; if $\mathfrak{P}$ is not principal, then there are just two j-invariants which are a conjugate pair over $\mathbb{F}_{p^2}$ such that their endomorphism rings correspond to this type. Hence, if j-invariant of E is defined over $\mathbb{F}_p$, then $\mathrm{Hom}(E^{(p)}, E)\phi_{p,E}$ is the unique principal prime ideal $\mathfrak{P}$ over p; if j-invariant of E is not defined over $\mathbb{F}_p$, then $\mathrm{Hom}(E^{(p)}, E)\phi_{p,E}$ is the unique two-sided prime ideal $\mathfrak{P}$ over p where $\mathfrak{P}$ is not principal and $\mathfrak{P}^2 = (p)$. Thus β corresponds to $\mathfrak{P}^e$.

If E is ordinary, then $\widehat{\phi_{p^n,E}}$ is separable and $\ker\widehat{\phi_{p^n,E}} = E[p^n]$ which is a cyclic group. Since the Kronecker symbol $(\frac{t^2-4q}{p}) = 1$, then p splits in $\mathrm{End}(E)$ and there are two prime ideals $\mathfrak{P}_1, \mathfrak{P}_2$ of norm p. Let $\mathfrak{P}_1$ be the one such that $\mathfrak{P}_1^n = (\pi_{p^n,E})$ where $q = p^n$, then $\mathfrak{P}_1 = \mathrm{Hom}(E^{(p)}, E)\phi_{p,E}$ and the other prime ideal $\mathfrak{P}_2 = \mathrm{Hom}(E, E^{(p)})\widehat{\phi}_{p,E} = \mathrm{Hom}(E^{(p^{n-1})}, E)\widehat{\phi}_{p,E^{(p^{n-1})}}$. Hence $\mathfrak{P}_1$ is the kernel ideal corresponding to $\phi_{p,E}$ and $\mathfrak{P}_2$ is the kernel ideal corresponding to $\widehat{\phi}_{p,E^{(p^{n-1})}}$. Let β be an isogeny from E with degree p^e and inseparable degree p^{e_1}, then β corresponds to $= \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e-e_1}$.

2.3. ℓ-isogeny graph

It is obvious that an ordinary curve and a supersingular curve can never be isogenous. So we can consider the ordinary case and the supersingular case respectively. Given a prime number ℓ, $\ell \neq p$, we introduce the isogeny graph in the following.

- Supersingular case: The ℓ-isogeny graph G_ℓ^s of supersingular elliptic curves over $\bar{k}$ where the vertices are the $\bar{k}$-isomorphism classes of elliptic curves and the directed edges correspond to the ℓ-isogenies, is a $\ell+1$ regular connected Ramanujan graph[5, 12] . Every vertex has $\ell+1$ out-degree. Consider the supersingular ℓ-isogeny graph $G_\ell^s(k,t)$ over k with trace t, where the vertices are the k-isomorphism classes of elliptic curves and the edges correspond to the l-isogenies defined over k. If all endomorphisms are defined over k, we have $G_\ell^s(\mathbb{F}_{p^n}, \pm 2p^{\frac{n}{2}}) \cong G_\ell^s[1]$. Otherwise, the ℓ-isogeny graphs over k are similar to the ordinary case. In fact, we might as well suppose that $k = \mathbb{F}_{p^2}$ since every supersingular j-invariant is defined over $\mathbb{F}_{p^2}$.

- Ordinary case: Let $G_\ell^o(k,t)$ be the ℓ-isogeny graph of ordinary elliptic curves defined over k with trace t. The structure of $G_\ell^o(k,t)$ was clear by the following three propositions from Kohel's thesis[9] and then Sutherland put forward the definition of ℓ-volcano[17]. Suppose $\mathbb{Z}[\pi_{q,E}]$ has conductor f_0, then $G_\ell^o(k,t)$ consists of finite such ℓ-volcanoes with $d = v_\ell(f_0)$ where v_ℓ is the ℓ-adic valuation. More precisely, the number of all vertices with endomorphism ring $\mathcal{O}$ is the ring class number $h(\mathcal{O})$[13, 17, 21]. Any two volcanoes can't be connected, otherwise

they are the same one. After enumerating the number of vertices in $G_\ell^o(k,t)$, $G_\ell^o(k,t)$ have $\sum_{\substack{\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K, \\ \mathcal{O} \text{ is maximal at } \ell}} \frac{h(\mathcal{O})}{ord_{cl(\mathcal{O})}(I)}$ connected components where $cl(\mathcal{O})$ is the ring class group and I is a prime ideal of $\mathcal{O}$ over ℓ.

Definition 2.1. *An ℓ-volcano V of level d is a connected undirected graph whose vertices are partitioned into $V_0, \ldots, V_d$ such that the followings hold:*

1) *The subgraph on V_0 (the surface) is a regular graph of degree at most 2.*

2) *For $i > 0$, each vertex in V_i has exactly one neighbor in level V_{i-1}, and this accounts for every edge not on the surface.*

3) *For $i < d$, each vertex in V_i has degree $\ell + 1$ and each vertex in V_d(the floor) has degree 1.*

Proposition 2.3. *Let E_2/k be ordinary, $\beta : E_2 \to E_1$ is an isogeny of prime degree ℓ prime to p, then the following three conditions will happen:*

1) *$\text{End}(E_1) \cong \text{End}(E_2)$, in which case we say that β is horizontal.*

2) *$[\text{End}(E_2) : \text{End}(E_1)] = \ell$, in which case we say that β is descending.*

3) *$[\text{End}(E_1) : \text{End}(E_2)] = \ell$, in which case we say that β is ascending.*

Proof. See [9, Proposition 21] or [17, Section 2.7]. $\square$

Note that for $[\text{End}(E_1) : \text{End}(E_2)] = \ell$, we may write $[\text{End}(E_2) : \text{End}(E_1)] = \frac{1}{\ell}$ for the same meaning in the following.

Proposition 2.4. *Let $\beta : E_2 \to E_1$ be an isogeny of ordinary elliptic curves over k, then the following conditions are equivalent:*

1) *$\text{End}(E_1)$ and $\text{End}(E_2)$ are isomorphic.*

2) *The left ideal $\text{Hom}(E_1, E_2)\beta$ is an invertible ideal of $\text{End}(E_2)$ with norm equal to $deg(\beta)$.*

3) *There exists an isogeny $\psi : E_2 \to E_1$ of degree relatively prime to $deg(\beta)$.*

Proof. See [9, Proposition 22] or [17, Section 2.9]. $\square$

Proposition 2.5. *Let E/k be an ordinary elliptic curve with endomorphism ring $\mathcal{O}$ of discriminant D, let ℓ be a prime different from p, and let $\left(\frac{*}{*}\right)$ be the Kronecker symbol. The following isogenies are defined over k.*

1) *If $\mathcal{O}$ is maximal at ℓ, then there are $1 + \left(\frac{D}{\ell}\right)$ isogenies of degree ℓ from E to curves with endomorphism ring $\mathcal{O}$.*

2) *If $\mathcal{O}$ is not maximal at ℓ, then there are no isogenies of degree ℓ from E to curves with endomorphism ring $\mathcal{O}$.*

3) *If there exist more than $1 + \left(\frac{D}{\ell}\right)$ distinct isogenies from E of degree ℓ then all isogenies from E of degree ℓ are defined over k, and up to k-isomorphism of E', there are exactly*

$$\left(l - \left(\frac{D}{\ell}\right)\right)[\mathcal{O}^* : \mathcal{O}'^*]^{-1}$$

elliptic curves E' and $[\mathcal{O}^* : \mathcal{O}'^*]$ distinct isogenies $E \to E'$ of degree ℓ such that $[\text{End}(E) : \text{End}(E')] = \ell$ where $\text{End}(E') = \mathcal{O}'$.

Proof. See [9, Proposition 23] or [17, Section 2.10]. $\square$

Note that $|\mathcal{O}^*| = 2$ if $j_E \neq 0, 1728$. If $j_E = 1728$, then $\text{End}(E) = \mathbb{Z}[i]$ and if $j_E = 0$, then $\text{End}(E) = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

2.4. Ideals of imaginary quadratic orders

This subsection can be found in [4, 6]. Suppose now K is an imaginary quadratic field, $\mathcal{O}$ is an order of it. An $\mathcal{O}$-ideal I is an additive subgroup of $\mathcal{O}$ which is an $\mathcal{O}$-module with respect to multiplication. I is called primitive if it cannot be written as tJ for some $t \in \mathbb{Z}$ and J is an $\mathcal{O}$-ideal. I is called proper if $\{\alpha \in K | \alpha I \subseteq I\} = \mathcal{O}$. I is invertible if and only if it is proper. Since $\mathrm{rank}_{\mathbb{Z}}(\mathcal{O}) = 2$, its ideals also have a basis consisting of two elements. Suppose K has discriminant D_0, and let γ be $\pm\frac{\sqrt{D_0}}{2}$ if $D_0 \equiv 0 \pmod 4$ or $\frac{1\pm\sqrt{D_0}}{2}$ if $D_0 \equiv 1 \pmod 4$. Suppose $\mathcal{O}$ has conductor f, then the discriminant of $\mathcal{O}$ is $f^2 D_0$. Any primitive $\mathcal{O}$-ideal I can be written as $\mathbb{Z}a + \mathbb{Z}(b + f\gamma)$[4, Proposition 8.4.5]. For the general integral ideals, they have the form $\mathbb{Z}at + \mathbb{Z}t(b + f\gamma)$ where $t, a \in \mathbb{Z}$. The norm of I in $\mathcal{O}$ is $[\mathcal{O} : I] = t^2 a$.

3. The index of $\mathrm{Hom}_k(E_1, E_2)\beta$ in $\mathrm{End}_k(E_2)$

Proposition 3.1. *Given two elliptic curves E_1, E_2 defined over a finite field k with the same trace, if $\mathrm{End}_k(E_2) = \mathrm{End}(E_2)$, then $\mathrm{Hom}_k(E_1, E_2) = \mathrm{Hom}(E_1, E_2)$.*

Proof. If $\mathrm{Hom}_k(E_1, E_2) \neq 0$, then $\mathrm{rank}_{\mathbb{Z}}\mathrm{Hom}_k(E_1, E_2) = \mathrm{rank}_{\mathbb{Z}}\mathrm{End}_k(E_2)$, since $\mathrm{Hom}_k(E_1, E_2)\beta$ is a non-zero ideal of $\mathrm{End}_k(E_2)$ for any non-zero $\beta \in \mathrm{Hom}_k(E_2, E_1)$. Since $\mathrm{Hom}_k(E_1, E_2) \subseteq \mathrm{Hom}(E_1, E_2)$ with the same rank as $\mathbb{Z}$-module, for any $\alpha \in \mathrm{Hom}(E_1, E_2)$, there exists $m \in \mathbb{Z}$ such that $m\alpha \in \mathrm{Hom}_k(E_1, E_2)$. If α is separable, since $\ker(m) \subseteq \ker(m\alpha)$, there exists $\alpha' \in \mathrm{Hom}_k(E_1, E_2)$ such that $m\alpha = \alpha'm$ by [14, Corollarly III 4.11], hence $\alpha = \alpha'$. If α is not separable with inseparable degree q', then α can be factored as $\alpha = \lambda\phi_{q', E_1}$ where λ is separable from $E_1^{(q')}$ to E_2. λ can be proved to be defined over k since $E_1^{(q')}$ is also defined over k, hence α is defined over k. $\square$

Hence for the elliptic curves over k whose endomorphisms are all defined over k, it is enough to consider $\mathrm{Hom}(E_1, E_2)$. In fact, with the help of the study of Waterhouse and Kohel, it is relatively simple to get the index of $\mathrm{Hom}(E_1, E_2)\beta$ in $\mathrm{End}(E_2)$ when E_2 is supersingular or E_2 is ordinary and $\mathrm{Hom}(E_1, E_2)\beta$ is an invertible ideal of $\mathrm{End}(E_2)$. But it is not trivial to get the answer for any β when E_2 is ordinary and $\mathrm{Hom}(E_1, E_2)\beta$ is not invertible.

3.1. Supersingular case

Theorem 3.1. *Given two supersingular elliptic curves E_1, E_2 defined over k, and an isogeny $\beta : E_2 \to E_1$, then*

$$[\mathrm{End}(E_2) : \mathrm{Hom}(E_1, E_2)\beta] = [\mathrm{End}(E_1) : \beta\mathrm{Hom}(E_1, E_2)] = (\deg\beta)^2$$

and $\mathrm{Hom}(E_1, E_2)\beta$ is the kernel ideal corresponding to β.

Proof. For every left(right) ideal I of a maximal order of $B_{p,\infty}$, the reduced norm of I can be defined as
$$\mathrm{Nrd}(I) = \gcd\{\mathrm{Nrd}(\alpha) : \alpha \in I\}.$$

Choose a prime ℓ prime to $\deg\beta$. Since the ℓ-isogeny graph is connected, there is an isogeny $\alpha_0 : E_1 \to E_2$ with degree ℓ-power. Hence

$$\mathrm{Nrd}(\mathrm{Hom}(E_1, E_2)\beta) = \gcd\{\deg(\alpha)\deg(\beta) : \alpha \in \mathrm{Hom}(E_1, E_2)\} = \deg(\beta).$$

Since the index of an left(right) ideal in a maximal order of the quaternion algebra is the square of the reduced norm of the ideal, we have

$$[\mathrm{End}(E_2) : \mathrm{Hom}(E_1, E_2)\beta] = [\mathrm{End}(E_1) : \beta\mathrm{Hom}(E_1, E_2)] = (\deg\beta)^2.$$

Since $\mathrm{H}(\beta) \subseteq \mathrm{H}(\mathrm{Hom}(E_1, E_2)\beta) \subseteq \mathrm{H}([\deg(\beta)])$ and $\mathrm{H}(\alpha_0\beta) \cap H([\deg\beta]) = \mathrm{H}(\beta)$, it follows that

$$\mathrm{H}(\mathrm{Hom}(E_1, E_2)\beta) = \mathrm{H}(\beta).$$

Hence $\mathrm{Hom}(E_1, E_2)\beta$ is the kernel ideal of β. $\square$

Remark 3.1. Kohel had proved that all ideals of $\text{End}(E_2)$ could be in form of $\text{Hom}(E_1, E_2)\beta$ in his thesis[9]. In fact, there is a one-to-one correspondence between the isogenies from E_2 and the left ideals of $\text{End}(E_2)$. Under this correspondence, the reduced norm of the ideal is equal to the degree of the corresponding isogeny.

If $\text{Hom}_k(E_1, E_2) \neq 0$ and $\text{End}_k(E_2)(\neq \text{End}(E_2))$ is isomorphic to an imaginary quadratic order, we can analyze it similarly to the ordinary case which is omitted here.

3.2. Ordinary case

In the following, we say an isogeny β doesn't have any backtracking if β can't be written as $m\beta'$ for some $m \in \mathbb{Z}$ and some isogeny β'. We assume E_1 and E_2 are ordinary, and let K be the endomorphism algebra of E_2, and denote its algebraic integer ring $\mathcal{O}_K$ by $\mathbb{Z} + \mathbb{Z}\gamma$. We begin with the following lemma and its corollary which guarantee the assumptions about the relations of the endomorphism rings in Lemma 3.3 and Theorem 3.2. Next we get the results for the isogenies of prime powers and finally use the results of the prime power case to prove the general case by the recurrence method.

Lemma 3.1. *Given two ordinary elliptic curves E_1, E_2 defined over k. If there is an isogeny between them of degree ℓ^e where $\ell \neq p$, then $[\text{End}(E_2) : \text{End}(E_1)] = \ell^{e'}$ where $|e'| \leqslant e$. Conversely, if $[\text{End}(E_2) : \text{End}(E_1)] = \ell^{e'}$, then the degree of every isogeny between them is divided by $\ell^{|e'|}$.*

Proof. Since distinct ℓ-volcanoes are unconnected, E_1 and E_2 must be in the same ℓ-volcano. Let $\beta : E_2 \to E_1$ be an isogeny of degree ℓ^e, β can be looked as a path walking in the ℓ-volcano since all ℓ-isogenies are represented as a edge in the ℓ-volcanoes. We may as well assume that β does not have backtracking, then the path can be showed as

$$E_0' := E_2 \xrightarrow{\beta_1} E_1' \xrightarrow{\beta_2} \cdots \xrightarrow{\beta_e} E_e' =: E_1$$

where $\ker\beta_i = \ell^{e-i}\beta_{i-1}\cdots\beta_1(\ker\beta)$ and β_i are also defined over k for all i. According to Proposition 2.3, $[\text{End}(E_i') : \text{End}(E_{i+1}')] = 0$, ℓ or ℓ^{-1} for all i. Hence $[\text{End}(E_2) : \text{End}(E_1)] = \ell^{e'}$ where $|e'| \leqslant e$.

Conversely, suppose $e' > 0$, then there is an elliptic curve E_2' with the same endomorphism ring with E_2 descending directly to E_1 such that every isogeny β between them must pass E_2'. Hence $\ell^{e'} \mid \deg\beta$. If $e' < 0$, consider $\widehat{\beta}$ and the lemma holds. One can also refer to [9, Proposition 5] for another proof. $\square$

Corollary 3.1. *Given two ordinary elliptic curves E_1, E_2 defined over k. If there is an isogeny between them of degree m with factorization $p^e \ell_1^{e_1} \cdots \ell_s^{e_s}$, then $[\text{End}(E_2) : \text{End}(E_1)]$ has the form $\ell_1^{e_1'} \cdots \ell_s^{e_s'}$ where $|e_i'| \leqslant e_i$ for all i. Conversely, if $[\text{End}(E_2) : \text{End}(E_1)]$ has the form $\ell_1^{e_1'} \cdots \ell_s^{e_s'}$, then the degree of every isogeny between them is divided by $\ell_1^{|e_1'|} \cdots \ell_s^{|e_s'|}$.*

Proof. Suppose the isogeny is $\beta : E_2 \to E_1$. Since $\ker\beta$ is a finite abelian group and can be a direct sum of subgroups of different prime powers. Let $\ker\beta = G_1 + \cdots + G_s + G_{s+1}$ where $|G_i| = \ell_i^{e_i}$ for $i < s + 1$ and $|G_{s+1}| \mid p^e$. Let

$$E_2 =: E_0' \xrightarrow{\beta_1} E_1' \xrightarrow{\beta_2} \cdots \xrightarrow{\beta_s} E_s' \xrightarrow{\beta_{s+1}} E_{s+1}' := E_1.$$

where $\ker\beta_i = \beta_{i-1}\cdots\beta_1 G_i$ and they are both defined over k. For every $i < s+1$, by Lemma 3.1, $[\text{End}(E_{i-1}') : \text{End}(E_i')] = \ell_i^{e_i'}$ where $|e_i'| \leqslant e_i$. Hence $[\text{End}(E_2) : \text{End}(E_1)]$ has the form $\ell_1^{e_1'} \cdots \ell_s^{e_s'}$ where $|e_i'| \leqslant e_i$ for all i, since $[\text{End}(E_s') : \text{End}(E_{s+1}')] = 0$.

Conversely, see [9, Proposition 5] or by Lemma 3.1. $\square$

Lemma 3.2. *Let $\beta : E_2 \to E_1$ be a separable isogeny of elliptic curves over k, then we have $I(\ker\beta) = \text{Hom}(E_1, E_2)\beta$.*

Proof. For any $\alpha \in I(\ker\beta)$, since $\ker\beta \subseteq \ker\alpha$ and β is separable, there exists $\lambda \in \text{Hom}(E_1, E_2)$ such that $\alpha = \lambda\beta$. Hence $I(\ker\beta) \subseteq \text{Hom}(E_1, E_2)\beta$. So $I(\ker\beta) = \text{Hom}(E_1, E_2)\beta$, since $\text{Hom}(E_1, E_2)\beta \subseteq I(\ker\beta)$ according to definition. $\square$

Lemma 3.3. *Given two ordinary elliptic curves E_1, E_2 defined over k and $\beta : E_2 \to E_1$ an isogeny of degree ℓ^e (ℓ can be p), and suppose $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell^{e'}$ where $|e'| \leqslant e$, then $[\mathrm{End}(E_2) : \mathrm{Hom}(E_1, E_2)\beta] = \ell^{e'}\deg\beta$ if $e' > 0$ or $\deg\beta$, otherwise. In addition, suppose $\mathrm{End}(E_2)$ has conductor f, writing $\mathrm{End}(E_2) = \mathbb{Z} + \mathbb{Z}f\gamma$, and $\beta = \ell^{e_0}\beta'$ where β' has no backtracking, then $\mathrm{Hom}(E_1, E_2)\beta = \mathbb{Z}\deg\beta + \mathbb{Z}\ell^{e_0+e'}(b + f\gamma)$ if $e' > 0$ and $\mathrm{Hom}(E_1, E_2)\beta = \mathbb{Z}\deg\beta + \mathbb{Z}\ell^{e_0}(\ell^{|e'|}b + f\gamma)$ where $\ell^{|e'|}|f$, otherwise.*

Proof. First, we assume β has no backtracking. If $\ell \neq p$, then β is separable, hence by Lemma 3.2, $\mathrm{Hom}(E_1, E_2)\beta = \mathrm{I}(\ker\beta)$. It is enough to prove for $e' \geq 0$. For $e' < 0$, we can consider the dual isogeny $\widehat{\beta}$ where $\mathrm{I}(\ker\widehat{\beta}) = \overline{\mathrm{I}(\ker\beta)}$ (note that $\bar{\gamma} = -\gamma$ or $-\gamma + 1$, so that $\overline{\mathrm{I}(\ker\beta)}$ can written like above).

Now assume $e' > 0$. Consider E_2 and E_1 in the ℓ-volcano, then there is an elliptic curve E_2' with the same endomorphism ring with E_2 descending directly to E_1 such that the path β must pass E_2'. Write $\beta = \beta_2\beta_1$ where $\beta_1 : E_2 \to E_2'$ and β_2 is the descending directly path from E_2' to E_1. If $e' = 0$, let $E_2' = E_1$ and $\beta_2 = id$.

Since β has no backtracking, $\ker\beta$ is a cyclic group of order ℓ^e. Since ℓ^e is the smallest integer belonging to $\mathrm{I}(\ker\beta)$, we have $\mathrm{I}(\ker\beta) \cap \mathbb{Z} = \mathbb{Z}\ell^e$. Let $\ker\beta = \langle P \rangle$. Similarly, $\ker\beta_1$ is a cyclic group of order $\ell^{e-e'}$, and $\ell^{e'}\beta_1 P = \infty$, then $\ker\beta_1 = \langle \ell^{e'}P \rangle$.

Since $\mathrm{End}(E_2) \cong \mathrm{End}(E_2')$, $\mathrm{I}(\ker\beta_1)$ is an invertible ideal of norm equal to $\deg\beta_1 = \ell^{e-e'}$ by Proposition 2.4. Similarly, it can be proved that $\mathrm{I}(\ker\beta_1) \cap \mathbb{Z} = \mathbb{Z}\ell^{e-e'}$, hence $\mathrm{I}(\ker\beta_1)$ has the form $\mathbb{Z}\ell^{e-e'} + \mathbb{Z}(b + f\gamma)$ for some $b \in \mathbb{Z}$. Since $\mathrm{I}(\ker\beta)$ is also an ideal of $\mathrm{End}(E_1)$, $\mathrm{I}(\ker\beta)$ is contained in $\mathbb{Z} + \mathbb{Z}\ell^{e'}f\gamma$. Since $\ell^{e'}(b + f\gamma)(P) = (b + f\gamma)(\ell^{e'}P) = \infty$, it follows that $\ell^{e'}(b + f\gamma) \in \mathrm{I}(\ker\beta)$. Hence $\mathrm{I}(\ker\beta) = \mathbb{Z}\ell^e + \mathbb{Z}\ell^{e'}(b + f\gamma)$ and $[\mathrm{End}(E_2) : \mathrm{I}(\ker\beta)] = \ell^{e'}\deg\beta$.

If $\ell = p$, then $\mathrm{End}(E_1) \cong \mathrm{End}(E_2)$ and $\mathrm{Hom}(E_1, E_2)\beta$ is an invertible ideal of norm $\deg\beta$ by Proposition 2.4, since $\mathbb{Z}[\pi_{q,E_2}]$ is maximal at p.

If β has backtracking, since $\mathrm{Hom}(E_1, E_2)\ell^{e_0}\beta' = \ell^{e_0}\mathrm{Hom}(E_1, E_2)\beta'$, the lemma holds. $\qquad\square$

Corollary 3.2. *Given ordinary elliptic curves E_1, E_2 defined over k where $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell^{e'}$, $\ell \neq p$, $e' \in \mathbb{Z}_{>0}$. Let $\beta : E_2 \to E_1$ be an isogeny without backtracking of prime power degree, and suppose $\mathrm{End}(E_2) = \mathbb{Z} + \mathbb{Z}f\gamma$, then $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}\widehat{\beta} + \mathbb{Z}\frac{\ell^{e'}(b+f\gamma)\widehat{\beta}}{\deg\beta}$ for some integer b. In addition, if $\deg\beta = \ell^{e'}$, then $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}\widehat{\beta} + \mathbb{Z}f\gamma\widehat{\beta}$.*

Proof. Since $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell^{e'}$, we have $\ell \mid \deg\beta$. By Lemma 3.3,

$$\mathrm{Hom}(E_1, E_2)\widehat{\beta} = \mathbb{Z}\deg\beta + \mathbb{Z}\ell^{e'}(\mathrm{b} + f\gamma)$$

for some integer b, then $\mathrm{Hom}(E_1, E_2) = \frac{\mathrm{Hom}(E_1, E_2)\beta\widehat{\beta}}{\deg\beta} = \mathbb{Z}\widehat{\beta} + \mathbb{Z}\frac{\ell^{e'}(b+f\gamma)\widehat{\beta}}{\deg\beta}$. If $\deg\beta = \ell^{e'}$, then b can be 0. $\qquad\square$

Corollary 3.3. *Given ordinary elliptic curves E_1, E_2 defined over k where $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell^{e'}$ where $e' \in \mathbb{Z}$. Then every isogeny from E_2 to E_1 can correspond to an ideal of $\mathrm{End}(E_2)$ if and only if $e' \leqslant 0$.*

Proof. If $e' = 0$, then $\mathrm{End}(E_1) \cong \mathrm{End}(E_2)$. Hence for any isogeny $\beta \in \mathrm{Hom}(E_2, E_1)$, β corresponds to the invertible ideal $\mathrm{Hom}(E_1, E_2)\beta$. Otherwise, $\ell \neq p$ and $\ell \mid \deg(\beta)$. Factor β as $\beta_2\beta_1$ where $\deg\beta_2$ is ℓ-power and $\ell \nmid \deg\beta_1$. Let E_3 be the target elliptic curve of β_1 where $\mathrm{End}(E_3) \cong \mathrm{End}(E_2)$.

If $e' < 0$, since

$$\ker(\beta_2) \subseteq \mathrm{H}(\mathrm{Hom}(E_1, E_3)\beta_2) \subseteq E_3[\deg\beta_2]$$

and $E_3[\ell] \nsubseteq \mathrm{H}(\mathrm{Hom}(E_1, E_3)\beta_2)$ by Lemma 3.3 (otherwise $\frac{f\gamma}{\ell} \in \mathrm{End}(E_3)$, which is a contradiction), we obtain $\mathrm{H}(\mathrm{Hom}(E_1, E_3)\beta_2) = \ker(\beta_2)$, hence $\mathrm{Hom}(E_1, E_3)\beta_2$ is the kernel ideal for β_2. So β can correspond to an ideal by Proposition 2.2, since β_1 can also correspond to an ideal.

If $e' > 0$, suppose that β has no backtracking. If β can correspond to some ideal, then $\beta\widehat{\beta_1} = \beta_2\deg\beta_1$ corresponds to an ideal. Hence β_2 corresponds to an ideal. By lemma 3.3, we have $E_3[\ell^{e'}] \subseteq \mathrm{H}(\mathrm{Hom}(E_1, E_3)\beta_2)$, then the isogeny corresponding to the kernel ideal $\mathrm{Hom}(E_1, E_3)\beta_2$ can be written as $\ell^{e'}\beta'$ for some isogeny β' from E_3, hence $\mathrm{Hom}(E_1, E_3)\beta_2$ isn't the kernel ideal for β_2 since β_2 has no backtracking. Let J be the kernel ideal of β_2 such that $\mathrm{H}(J) = \mathrm{H}(\beta_2)$, then

$J = \mathrm{I}(\mathrm{H}(J)) = \mathrm{I}(\ker(\beta_2)) = \mathrm{Hom}(E_1, E_3)\beta_2$ since β_2 is separable. Thus we obtain a contradiction. β can not correspond to an ideal.

$\square$

Now take out the condition that the degrees of the isogenies are prime powers. For simplicity, we define $\rho(e)$ as

$$\rho(e) = \begin{cases} e, \text{ if } e > 0. \\ 0, \text{ otherwise.} \end{cases}$$

Theorem 3.2. *Given two ordinary elliptic curves E_1, E_2 defined over k and $\beta : E_2 \to E_1$ an isogeny of degree m, let the prime factorization of m be $p^e \ell_1^{e_1} \cdots \ell_s^{e_s}$ where $e \in \mathbb{Z}_{\geqslant 0}$ and $e_i \in \mathbb{Z}_{>0}$. Suppose $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell_1^{e_1'} \cdots \ell_s^{e_s'}$ where $|e_i'| \leqslant e_i$ for all i, then*

$$[\mathrm{End}(E_2) : \mathrm{Hom}(E_1, E_2)\beta] = \prod_{i=1}^{s} \ell_i^{\rho(e_i')} \deg\beta.$$

In addition, suppose $\mathrm{End}(E_2)$ has conductor f, writing $\mathrm{End}(E_2) = \mathbb{Z} + \mathbb{Z}f\gamma$, and $\beta = m'\beta'$ where $m' \in \mathbb{Z}$ and β' has no backtracking, then

$$\mathrm{Hom}(E_1, E_2)\beta = m'(\mathbb{Z}\deg\beta' + \mathbb{Z}\prod_{i=1}^{s} \ell_i^{\rho(e_i')}(b \prod_{i=1}^{s} \ell_i^{\rho(e_i')-e_i'} + f\gamma))$$

for some integer b where $\prod_{i=1}^{s} \ell_i^{\rho(e_i')-e_i'} \mid f$.

Proof. Similarly, it is enough to prove the case β has no backtracking. If β has inseparable degree p^e and $e > 0$, then we factor β as

$$E_2 \overset{\phi_{p^e, E_2}}{\longrightarrow} E_2^{(p^e)} \overset{\lambda}{\longrightarrow} E_1$$

where λ is separable of degree $\ell_1^{e_1} \cdots \ell_s^{e_s}$. We consider $\widehat{\beta} = \widehat{\phi}_{p^e, E_2}\widehat{\lambda}$ and $\mathrm{Hom}(E_2, E_1)\widehat{\beta}$ instead. Assume β is separable, let β be factored as $\beta_{s+1} \cdots \beta_2\beta_1$ where $\deg\beta_i = \ell_i^{e_i}$ and $\deg\beta_{s+1} = p^e$ as in the proof of Corollary 3.1. So we have

$$E_2 \overset{\beta_1}{\to} E_1' \overset{\beta_2}{\to} \cdots \overset{\beta_s}{\to} E_s' \overset{\beta_{s+1}}{\to} E_{s+1}' := E_1.$$

In the following, we prove the theorem recursively.

Suppose $\mathrm{End}(E_2) = \mathbb{Z} + \mathbb{Z}f\gamma$, let $\ell_{s+1} = p$ and $e_{s+1} = e$, then

$$\mathrm{End}(E_i') = \mathbb{Z} + \mathbb{Z}\ell_1^{e_1'} \cdots \ell_i^{e_i'}f\gamma$$

for all i and $e_{s+1}' = 0$. We claim that $\mathrm{Hom}(E_i', E_2)\beta_i \cdots \beta_1$ has the form

$$\mathbb{Z}\prod_{j=1}^{i} \ell_j^{e_j} + \mathbb{Z}\prod_{j=1}^{i} \ell_j^{\rho(e_j')}(b \prod_{j=1}^{i} \ell_j^{\rho(e_j')-e_j'} + f\gamma)$$

for some integer b.

Since β has no backtracking, every $\ker\beta_i$ and $\ker\beta$ are cyclic. Let $\ker\beta = \langle P \rangle$, then

$$\ker(\beta_i \cdots \beta_1) = \langle \prod_{j=i+1}^{s+1} \ell_j^{e_j} P \rangle.$$

Hence we have $\mathrm{I}(\ker(\beta_i \cdots \beta_1)) \cap \mathbb{Z} = \mathbb{Z}\prod_{j=1}^{i} \ell_j^{e_j}$, since $\ker(\beta_i \cdots \beta_1)$ is a cyclic group of order $\prod_{j=1}^{i} \ell_j^{e_j}$.

We also have $\mathrm{I}(\ker(\beta_i \cdots \beta_1)) \subseteq (\mathrm{End}(E_2) \cap \mathrm{End}(E_i')) = \mathbb{Z} + \mathbb{Z}\prod_{j=1}^{i} \ell_j^{\rho(e_j')}f\gamma$ where $\prod_{j=1}^{i} \ell_j^{\rho(e_j')-e_j'} \mid f$.

9

When $i = 1$, by Lemma 3.3, $\mathrm{Hom}(E_1', E_2)\beta_1$ has the form

$$\mathbb{Z}\deg\beta_1 + \mathbb{Z}\ell_1^{\rho(e_1')}(\ell_1^{\rho(e_1')-e_1'}b + f\gamma)$$

for some integer b. It holds.

If $\mathrm{Hom}(E_i', E_2)\beta_i \cdots \beta_1$ has the form $\mathbb{Z}\prod\limits_{j=1}^{i}\ell_j^{e_j} + \mathbb{Z}\prod\limits_{j=1}^{i}\ell_j^{\rho(e_j')}(b\prod\limits_{j=1}^{i}\ell_j^{\rho(e_j')-e_j'} + f\gamma)$ for some integer b, we consider $\mathrm{Hom}(E_{i+1}', E_2)\beta_{i+1} \cdots \beta_1$. Since $\mathrm{I}(\ker(\beta_{i+1} \cdots \beta_1))$ is an ideal of $\mathbb{Z} + \mathbb{Z}f\gamma$ and $\mathrm{I}(\ker(\beta_{i+1} \cdots \beta_1)) \cap \mathbb{Z} = \mathbb{Z}\prod\limits_{j=1}^{i+1}\ell_j^{e_j}$, $\mathrm{I}(\ker(\beta_{i+1} \cdots \beta_1))$ has the form $\mathbb{Z}\prod\limits_{j=1}^{i+1}\ell_j^{e_j} + \mathbb{Z}t(b' + f\gamma)$ for some integers t and b', where $t \mid \prod\limits_{j=1}^{i+1}\ell_j^{e_j}$. Since $\mathrm{I}(\ker(\beta_{i+1} \cdots \beta_1)) \subseteq \mathbb{Z} + \mathbb{Z}\prod\limits_{j=1}^{i+1}\ell_j^{\rho(e_j')}f\gamma$, we have $\prod\limits_{j=1}^{i+1}\ell_j^{\rho(e_j')} \mid t$. Let $t' := t/(\prod\limits_{j=1}^{i+1}\ell_j^{\rho(e_j')})$, then $\mathrm{I}(\ker(\beta_{i+1} \cdots \beta_1))$ has the form

$$\mathbb{Z}\prod_{j=1}^{i+1}\ell_j^{e_j} + \mathbb{Z}t'\prod_{j=1}^{i+1}\ell_j^{\rho(e_j')}(b' + f\gamma).$$

Since $\ell_{i+1}^{e_{i+1}}\prod\limits_{j=1}^{i}\ell_j^{\rho(e_j')}(\prod\limits_{j=1}^{i}\ell_j^{\rho(e_j')-e_j'}b + f\gamma)(\prod\limits_{j=i+2}^{s+1}\ell_j^{e_j}P) = \infty$, it follows that

$$\ell_{i+1}^{e_{i+1}}\prod_{j=1}^{i}\ell_j^{\rho(e_j')}(b\prod_{j=1}^{i}\ell_j^{\rho(e_j')-e_j'} + f\gamma) \in \mathrm{I}(\ker(\beta_{i+1} \cdots \beta_1)),$$

hence $t' \mid \ell_{i+1}^{e_{i+1}}$ and $\prod\limits_{j=1}^{i}\ell_j^{\rho(e_j')-e_j'} \mid b'$.

On the other hand, consider

$$\mathrm{Hom}(E_2, E_{i+1}')(\widehat{\beta_{i+1} \cdots \beta_1}) = \mathbb{Z}\prod_{j=1}^{i+1}\ell_j^{e_j} + \mathbb{Z}t'\prod_{j=1}^{i+1}\ell_j^{\rho(e_j')}(b' + f\bar{\gamma}).$$

(note that $\widehat{\beta_{i+1} \cdots \beta_1}$ may be inseparable when $i = s$, so we don't use symbol like $\mathrm{I}(\ker\beta)$)here.) Similarly, by Lemma 3.3, $\mathrm{Hom}(E_i', E_{i+1}')\widehat{\beta_{i+1}}$ has the form

$$\mathbb{Z}\ell_{i+1}^{e_{i+1}} + \mathbb{Z}\ell_{i+1}^{\rho(e_{i+1}')}(\ell_{i+1}^{\rho(e_{i+1}')-e_{i+1}'}b'' + \prod_{j=1}^{i}\ell_j^{e_j}f\bar{\gamma})$$

for some integer b''. Let $\ker(\widehat{\beta_{i+1} \cdots \beta_1}) = \langle Q \rangle$, then $\ker(\widehat{\beta_i \cdots \beta_1}) = \langle \widehat{\beta_{i+1}}(Q) \rangle$ is a cyclic group of order $\ell_1^{e_1} \cdots \ell_i^{e_i}$. Write $\ell_{i+1}^{\rho(e_{i+1}')}(\ell_{i+1}^{\rho(e_{i+1}')-e_{i+1}'}b'' + \prod\limits_{j=1}^{i}\ell_j^{e_j}f\bar{\gamma}) = \alpha\widehat{\beta_{i+1}}$ for some $\alpha \in \mathrm{Hom}(E_i', E_{i+1}')$, then we have $\ell_1^{e_1} \cdots \ell_i^{e_i}\alpha\widehat{\beta_{i+1}}(Q) = \infty$. If $i \neq s$, then $\widehat{\beta_{i+1} \cdots \beta_1}$ is separable, and we have

$$\ell_1^{e_1} \cdots \ell_i^{e_i}\ell_{i+1}^{\rho(e_{i+1}')}(\ell_{i+1}^{\rho(e_{i+1}')-e_{i+1}'}b'' + \prod_{j=1}^{i}\ell_j^{e_j}f\bar{\gamma}) \in \mathrm{Hom}(E_2, E_{i+1}')(\widehat{\beta_{i+1} \cdots \beta_1}),$$

hence $t' \mid \ell_1^{e_1} \cdots \ell_i^{e_i}$ and $\ell_{i+1}^{\rho(e_{i+1}')-e_{i+1}'} \mid b'$. Thus $t' = 1$. If $i = s$, then $\mathrm{End}(E_s') \cong \mathrm{End}(E_{s+1}')$ and there is an isogeny α' from E_{s+1}' to E_s' of degree prime to ℓ_{s+1}. We have

$$\alpha'\alpha\ell_1^{e_1} \cdots \ell_s^{e_s} \in \mathrm{I}(\ker(\widehat{\beta_s \cdots \beta_1})).$$

Since $\mathrm{I}(\ker(\widehat{\beta_s \cdots \beta_1})) = \mathrm{Hom}(E_2, E_s')\widehat{\beta_s \cdots \beta_1}$, it follows that

$$\widehat{\alpha'}\alpha'\alpha\ell_1^{e_1} \cdots \ell_s^{e_s}\widehat{\beta_{s+1}} \in \mathrm{Hom}(E_2, E_{s+1}')(\widehat{\beta_{s+1} \cdots \beta_1})$$

i.e.

$$\deg\alpha'\ell_1^{e_1}\cdots\ell_s^{e_s}\ell_{s+1}^{\rho(e'_{s+1})}(b''+\prod_{j=1}^{s}\ell_j^{e'_j}f\bar\gamma)\in\mathbb{Z}\prod_{j=1}^{s+1}\ell_j^{e_j}+\mathbb{Z}t'\prod_{j=1}^{s+1}\ell_j^{\rho(e'_j)}(b'+f\bar\gamma).$$

Hence $t'\mid\deg\alpha'\ell_1^{e_1}\cdots\ell_s^{e_s}$. Thus $t'=1$.

$\square$

Corollary 3.4. *Given ordinary elliptic curves E_1,E_2 defined over k where $[\mathrm{End}(E_2):\mathrm{End}(E_1)]=\ell_1^{e'_1}\cdots\ell_s^{e'_s}$ for different primes ℓ_i and $e'_i\in\mathbb{Z}_{\neq0}$. Let $\beta:E_2\to E_1$ be an isogeny without backtracking, suppose $\mathrm{End}(E_2)=\mathbb{Z}+\mathbb{Z}f\gamma$, then*

$$\mathrm{Hom}(E_1,E_2)=\mathbb{Z}\widehat\beta+\mathbb{Z}(\prod_{i=1}^{s}\ell_i^{\rho(e'_i)}(b\prod_{i=1}^{s}\ell_i^{\rho(e'_i)-e'_i}+f\gamma)\widehat\beta)/(\deg\beta)$$

for some integer b.

Proof. Similar to the proof of Corollary 3.2.

$\square$

Corollary 3.5. *Given ordinary elliptic curves E_1,E_2 defined over k where $[\mathrm{End}(E_2):\mathrm{End}(E_1)]=\ell_1^{e'_1}\cdots\ell_s^{e'_s}$ for different primes ℓ_i and $e'_i\in\mathbb{Z}_{\neq0}$ Then every isogeny from E_2 to E_1 can correspond to an ideal of $\mathrm{End}(E_2)$ if and only if all $e'_i\leqslant0$.*

Proof. Given any $\beta\in\mathrm{Hom}(E_2,E_1)$. If all $e'_i\leqslant0$, factor β as $\beta_r\cdots\beta_2\beta_1$ for some integer r and $\beta_1,\ldots,\beta_r$ are isogenies of distinct prime power degrees. By Corollary 3.3, every β_i can correspond to an ideal, then β can correspond to an ideal.

If there exists some i such that $e'_i>0$. Factor β as $\beta_2\beta_1$ where $\deg\beta_1$ is p-power and $\deg\beta_2$ is prime to p. Then β_2 is separable. It can be proved similarly with the proof of Corollary 3.3 that β can not correspond to an ideal. $\square$

According to Theorem 3.1 and Corollary 3.5, whether an isogeny can correspond to a kernel ideal is only up to the two elliptic curves, more precisely, up to their endomorphism rings.

4. The non-trivial minimal degree

Let $\mathrm{Md}_k(E_2,E_1):=\min\{\deg\beta:\beta\in\mathrm{Hom}_k(E_2,E_1),\deg\beta\neq1\}$, $\mathrm{Md}_k(E):=\mathrm{Md}_k(E,E)$, $\mathrm{Md}(E_2,E_1):=\mathrm{Md}_{\bar k}(E_2,E_1),\mathrm{Md}(E):=\mathrm{Md}_{\bar k}(E)$. Obviously, $\mathrm{Md}_k(E_2,E_1)=\mathrm{Md}_k(E_1,E_2)$. We call it the non-trivial minimal degree.

First we consider $\mathrm{Md}(E)$. It suffices to check whether E has an endomorphism of degree 2 or 3, since $2\in\mathrm{End}(E)$. We need to check this with the help of the Deuring's lifting theorem[7, 10].

Theorem 4.1. *Let E be an elliptic curve defined over a finite field and let α be an endomorphism of E. Then there exists an elliptic curve $\widetilde E$ defined over a finite extension H of $\mathbb{Q}$ and an endomorphism $\widetilde\alpha$ of $\widetilde E$ s.t. E is the reduction of $\widetilde E$ modulo some prime ideal of the ring of algebraic integers of K and the reduction of $\widetilde\alpha$ is α.*

In fact, $\deg\widetilde\alpha=\deg\alpha$. We lift α to $\widetilde\alpha$. Since $\widetilde\alpha\in\mathrm{End}(\widetilde E)$ has degree 2 or 3, $\widetilde\alpha$ corresponds to an element of some imaginary quadratic order of norm 2 or 3 respectively. However, the number of the imaginary quadratic orders containing elements of norm 2 or 3 are finite. Those with norm 2 are $\mathbb{Z}[\sqrt{-1}],\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, and those with norm 3 are $\mathbb{Z}[\sqrt{-2}],\mathbb{Z}[\frac{1+\sqrt{-3}}{2}],\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$. Since $1+\sqrt{-2}\in\mathrm{End}(E)$ implies $\sqrt{-2}\in\mathrm{End}(E)$, then we take out $\mathbb{Z}[\sqrt{-2}]$ when considering whether $\mathrm{Md}(E)=3$. For an imaginary quadratic order $\mathbb{Z}[\tau]$, let $j(\tau)$ denote the j-invariant of elliptic curve (over $\mathbb{C}$) having endomorphism ring by $\mathbb{Z}[\tau]$. Luckily, the above $j(\tau)$ of the above orders had been given out and there are elliptic curves over $\mathbb{Q}$ with the j-invariants[6, 15]. Let Δ_E be the discriminant of elliptic curve E.

τ	$j(\tau)$	minimal Weierstrass equation of E over $\mathbb{Q}$	Δ_E
$\sqrt{-1}$	$12^3 = 1728$	$y^2 = x^3 + x$	2^6
$\sqrt{-2}$	20^3	$y^2 = x^3 + 4x^2 + 2x$	2^9
$\frac{1+\sqrt{-7}}{2}$	-15^3	$y^2 + xy = x^3 - x^2 - 2x - 1$	7^3
$\frac{1+\sqrt{-3}}{2}$	0	$y^2 + y = x^3$	3^3
$\sqrt{-3}$	$2^4 3^3 5^3$	$y^2 = x^3 - 15x + 22$	$2^8 3^3$
$\frac{1+\sqrt{-11}}{2}$	-32^3	$y^2 + y = x^3 - x^2 - 7x + 10$	11^3

Table 1

Note that all $j(\tau) \in \mathbb{Z}$, then $j(\tau) \in \mathbb{F}_p$ after reduction. To make things more clearly, we still give out the results of supersingular case and ordinary case respectively. Coming back to the elliptic curves over finite fields, we also need Deuring's reduction theorem.

Theorem 4.2. *Let E be an elliptic curve over a number field H with $\mathrm{End}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an order of an imaginary quadratic field K. Let $\mathfrak{P}$ be prime ideal of H over p, where E has non-degenerate reduction $\bar{E}$. Then $\bar{E}$ is supersingular if and only if p doesn't split in K.*

Proof. See [10, Chapter 13, Theorem 12]. $\square$

Hence we have

Theorem 4.3. *Let E be a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$ with invariant j, then $\mathrm{Md}(E) = 2$ only when it satisfies one of the following conditions:*
(1) $j = 0$ when $p = 2, 3$;
(2) $j = 1728$ when $p \equiv 3 \pmod 4$;
(3) $j = 2^6 5^3$ when $p \equiv 5, 7 \pmod 8$;
(4) $j = -3^3 5^3$ when $p \equiv 3, 5, 6 \pmod 7$;
and $\mathrm{Md}(E) = 3$ only when it satisfies one of the following conditions:
(5) $j = 0$ when $p \equiv 2 \pmod 3$ and $p \neq 2, 5$;
(6) $j = 2^4 3^3 5^3$ when $p \equiv 2 \pmod 3$ and $p \neq 2, 5, 11, 17, 23$;
(7) $j = -2^{15}$ when $p \equiv 2, 6, 7, 8, 10 \pmod{11}$ and $p \neq 2, 7, 13, 17, 19$.
For other cases, $\mathrm{Md}(E) = 4$.

Proof. If $\alpha \in \mathrm{End}(E)$ has degree 2, then by Theorem 4.1, E and α can be lifted to $\widetilde{E}$ over some number field H and $\widetilde{\alpha}$ where $\deg \widetilde{\alpha} = 2$. Then $\widetilde{\alpha}$ can be $1 + \sqrt{-1}, \sqrt{-2}$ or $\frac{1+\sqrt{-7}}{2}$ where $\mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ are both maximal, hence $\mathrm{End}(\widetilde{E})$ is $\mathbb{Z}[\widetilde{\alpha}]$. Thus $j_{\widetilde{E}}$ is $1728, 2^6 5^3$ or $-3^3 5^3$ respectively. Although $\widetilde{E}$ may not be defined over $\mathbb{Q}$, there are elliptic curves defined over $\mathbb{Q}$ with the same j-invariant as $\widetilde{E}$. Suppose $\widetilde{E}$ is defined over $\mathbb{Q}$, just as those listed in Table 1. Then by Theorem 4.2, for proper p, $\widetilde{E}$ has non-degenerate reduction modulo p and becomes supersingular after reduction with the same j-invariant as E.

It is similar for case $\mathrm{Md}(E) = 3$. Notice that E may have both endomorphisms of degree 2 and 3, at that time $\mathrm{Md}(E) = 2$, that is why p can't be some values for the case $\mathrm{Md}(E) = 3$. $\square$

Remark 4.1. : For the supersingular elliptic curves defined over $\mathbb{F}_{p^n}$ with not all endomorphisms defined over $\overline{\mathbb{F}}_{p^n}$. We can get $\mathrm{Md}_{\mathbb{F}_{p^n}}(E)$ easily by some computations according to the possible conditions listed by Waterhouse [21, Theorem 4.1]. We don't list them here.

Theorem 4.4. *Let E be an ordinary elliptic curve defined over $\overline{\mathbb{F}}_p$ with invariant j, then $\mathrm{Md}(E) = 2$ only when it satisfies one of the following conditions:*
*(1) $j = 1728$ when $p \equiv 1 \pmod 4$;*
(2) $j = 2^6 5^3$ when $p \equiv 1, 3 \pmod 8$;
(3) $j = -3^3 5^3$ when $p \equiv 1, 2, 4 \pmod 7$;
and $\mathrm{Md}(E) = 3$ only when it satisfies one of the following conditions:
(4) $j = 0$ when $p \equiv 1 \pmod 3$;
(5) $j = 2^4 3^3 5^3$ when $p \equiv 1 \pmod 3$
(6) $j = -2^{15}$ when $p \equiv 1, 3, 4, 5, 9 \pmod{11}$.
For other cases, $\mathrm{Md}(E) = 4$.

Proof. Similar to the proof of the supersingular case. ☐

Given two ordinary elliptic curves E_1, E_2 defined over k where $E_1 \not\cong E_2$ and $\mathrm{Hom}(E_2, E_1) \neq 0$. If $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell^{e'}$ where $e' > 0$, and suppose E_1 and E_2 are in the same ℓ-volcano. If E_2 is above E_1 directly, then by Lemma 3.1, $\mathrm{Md}(E_2, E_1) = \ell^{e'}$. Otherwise, $\ell^{e'} \mid \mathrm{Md}(E_2, E_1)$ but they are not equal. Let E_3 be the elliptic curve directly above E_1 and E_2 with largest level. Suppose $[\mathrm{End}(E_3) : \mathrm{End}(E_2)] = \ell^{e''}$ where $e'' > 0$. The path from E_2 ascending to E_3 and then descending to E_1 corresponds to the isogeny of ℓ-power degree from E_2 to E_1 without backtracking or endomorphism cycles and it is the shortest path from E_2 to E_1 in the l-volcano. Let E_2' be the elliptic curve directly above E_1, if $\mathrm{Md}(E_2, E_2') = \ell^{2e''}$, then $\mathrm{Md}(E_2, E_1) = \ell^{e'+2e''}$. But it does not always hold.

Example 1. Let $k = \mathbb{F}_{41}$, $t = 6$, and $\ell = 2$. For simplicity, the k-isomorphism classes of elliptic curves with trace t are represented by their j-invariants in the following. Because the number of the k-isomorphism classes of elliptic curves with the same j-invariant is 2 for the j-invariants not equal to 0 or 1728 [3, Theorem 2.2] and the two k-isomorphism classes are twist of each other with their traces being opposite numbers. Here is the volcano we are considering.
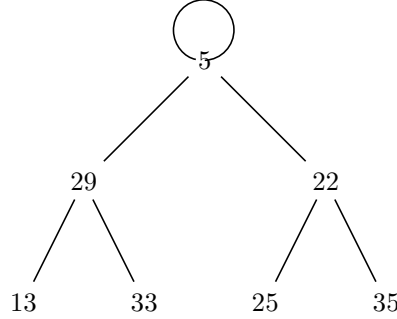
Let $j(E_2) = 29$, $j(E_1) = 25$ and $j(E_2') = 22$, then $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = 2$ and $\mathrm{Md}(E_2', E_1) = 2$. Since it can be checked by the modular equation [10, Chapter 5, Theorem 5] of order 3 that there is an isogeny from E_2 to E_3' of degree 3, then $\mathrm{Md}(E_2, E_2') = 3 \neq 2^2$. Hence $\mathrm{Md}(E_2, E_1) = 6$.

More generally, if $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell^{e'}$ where $e' > 0$, then there is E_2' directly above E_1 such that $\mathrm{End}(E_2) \cong \mathrm{End}(E_2')$. In this case, $\mathrm{Md}(E_2, E_1) = \mathrm{Md}(E_2, E_2')\ell^{e'}$ still holds. Thus this problem can be reduced to the case $\mathrm{End}(E_2) \cong \mathrm{End}(E_2')$. To get an upper bound for $\mathrm{Md}(E_2, E_2')$, we need the following lemma.

Lemma 4.1. *Let $\mathcal{O}$ be an imaginary quadratic order, then every invertible ideal class of $\mathcal{O}$ contains an ideal J with*

$$\|J\| \leqslant \frac{2}{\pi}\sqrt{|\mathrm{disc}(\mathcal{O})|}.$$

Proof. See [11, Chapter 5]. The proof is given there for the algebraic integer rings of number fields with the aid of Minkowski's theorem. It is easy to check that the proof still holds for imaginary quadratic orders. In fact, a proof for general orders of number rings is given by [16, Theorem 5.4]. ☐

Theorem 4.5. *Given two ordinary elliptic curves E_1, E_2 over $\mathbb{F}_q$ with trace t and they are not $\mathbb{F}_q$-isomorphic. Then*

$$\mathrm{Md}(E_2, E_1) \leqslant \frac{2}{\pi}(4q - t^2)^{\frac{1}{2}}.$$

Proof. Suppose $\mathbb{Z}[\pi_{q,E_2}] = \mathbb{Z} + \mathbb{Z}f_0\gamma$ with conductor $f_0 = \prod_{i=1}^{r} \ell_i^{e_i}$. And suppose $\mathrm{End}(E_1)$ $(\mathrm{End}(E_2))$ has conductor $f_1 = \prod_{i=1}^{r} \ell_i^{e_i'}$ $(f_2 = \prod_{i=1}^{r} \ell_i^{e_i''})$ where $0 \leqslant e_i'(e_i'') \leqslant e_i$ for all i. Then there are E_1', E_2' whose endomorphism rings have conductor $f = \prod_{i=1}^{r} \ell_i^{\min(e_i', e_i'')}$ such that $\mathrm{Md}(E_1, E_1') = \prod_{i=1}^{r} \ell_i^{e_i'-\min(e_i', e_i'')}$

and $\mathrm{Md}(E_2, E_2') = \prod_{i=1}^{r} \ell_i^{e_i'' - \min(e_i', e_i'')}$. Hence

$$
\begin{aligned}
\mathrm{Md}(E_1, E_2) &\leqslant \mathrm{Md}(E_1', E_2')\mathrm{Md}(E_1, E_1')\mathrm{Md}(E_2, E_2') \\
&\leqslant \frac{2}{\pi}\sqrt{\frac{4q - t^2}{\prod_{i=1}^{r} \ell_i^{2(e_i - \min(e_i', e_i''))}}(\prod_{i=1}^{r} \ell_i^{e_i' - \min(e_i', e_i'')})(\prod_{i=1}^{r} \ell_i^{e_i'' - \min(e_i', e_i'')})} \text{ (by Lemma4.1)} \\
&= \frac{2}{\pi}\sqrt{(4q - t^2)\prod_{i=1}^{r} \ell_i^{2(e_i' + e_i'' - e_i - \min(e_i', e_i''))}} \\
&\leqslant \frac{2}{\pi}(4q - t^2)^{\frac{1}{2}}.
\end{aligned}
$$

$\square$

The result in Theorem 4.5 is rough. For two elliptic curves with known endomorphism rings, the result can be more precise.

Example 2. Let $\mathrm{eB}(k, t)$ denote the upper bound given by Theorem 4.5, and $\mathrm{rB}(k, t)$ denote the largest non-trivial minimal degree in the k-isogenous class with trace t.

As in Example 1, let $k = \mathbb{F}_{41}$, $t = 6$, we have $\mathrm{eB}(\mathbb{F}_{41}, 6) = 7$. The 3-isogeny garph is
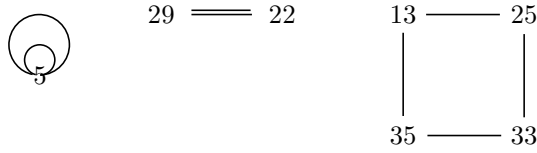
Then $\mathrm{rB}(\mathbb{F}_{41}, 6) = 6$.

Similarly, let $k = \mathbb{F}_{53}$, $t = -4$, we have $\mathrm{eB}(\mathbb{F}_{53}, -4) = 8$ and $\mathrm{rB}(\mathbb{F}_{53}, -4) = 7$. Let $k = \mathbb{F}_{67}$, $t = 12$, we have $\mathrm{eB}(\mathbb{F}_{67}, 12) = 7$ and $\mathrm{rB}(\mathbb{F}_{67}, 12) = 5$.

Theorem 4.6. *Given two supersingular elliptic curves E_1, E_2 over $\mathbb{F}_{p^2}$. Then $\mathrm{Md}(E_2, E_1) \sim O(p)$ and $\mathrm{Md}_{\mathbb{F}_{p^2}}(E_2, E_1) \sim O(p)$. If E_1, E_2 can be defined over $\mathbb{F}_p$ and they are not $\mathbb{F}_p$-isomorphic, then $\mathrm{Md}_{\mathbb{F}_p}(E_2, E_1) \leqslant \frac{4}{\pi}p^{\frac{1}{2}}$.*

Proof. As a result of [9, Theorem 79], $\mathrm{Md}(E_2, E_1) \sim O(p)$. If the trace is $\pm 2p$, then $\mathrm{Md}_{\mathbb{F}_{p^2}}(E_2, E_1)$ $= \mathrm{Md}(E_2, E_1)$. If the trace is not $\pm 2p$ and they are not $\mathbb{F}_{p^2}$-isomorphic, then $\mathrm{Md}_{\mathbb{F}_{p^2}}(E_2, E_1) = p[1]$. If E_1, E_2 can be defined over $\mathbb{F}_p$, by Lemma 4.1, we get $\mathrm{Md}_{\mathbb{F}_p}(E_2, E_1) \leqslant \frac{4}{\pi}p^{\frac{1}{2}}$. $\square$

Example 3. Let $p = 53$, then $\mathrm{eB}(\mathbb{F}_{53}, 0) = 9$. There is only one order $\mathcal{O}$ with discriminant $-2^2 53$ and it has ring class number 6. There are totally six $\mathbb{F}_{53}$-isomorphism classes and one j-invariant correspond to two $\mathbb{F}_{53}$-isomorphism classes. Denote them by $E(0, 1), E(0, 2), E(-3, 1), E(-3, 2)$, $E(-7, 1), E(-7, 2)$. The 2-isogeny graph is

$$\text{E(0,1) — E(-7,1)} \quad \text{E(-3,1) — E(-3,2)} \quad \text{E(0,2) — E(-7,2)}$$

And the 3-isogeny graph is

Then $\mathrm{rB}(\mathbb{F}_{53}, 0) = 6$. The five non-principal ideal classes in ring class group $cl(\mathcal{O})$ can be represented by one ideal of norm 2, two ideals of norm 3 and two ideals of norm 6.

References

References

[1] Gora Adj, Omran Ahmadi, and Alfred Menezes. On isogeny graphs of supersingular elliptic curves over finite fields. *Finite Fields and Their Applications*, 55:268–283, 2019.

[2] Reza Azarderakhsh, Matthew Campagna, Craig Costello, LD Feo, Basil Hess, Amir Jalali, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, et al. Supersingular isogeny key encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 2017.

[3] Reinier Bröker. *Constructing elliptic curves of prescribed order*. PhD thesis, Universiteit Leiden, 2006.

[4] Johannes Buchmann and Ulrich Vollmer. *Binary Quadratic Forms: An Algorithmic Approach*, volume 20. Springer, Berlin, 2007.

[5] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, 2009.

[6] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 1989.

[7] Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkrper. *In Abhandlungen aus dem mathematischen Seminar der Universitt Hamburg*, 14(1):197–272, 1941.

[8] Steven D Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–33. Springer, 2017.

[9] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.

[10] Serge Lang. *Elliptic functions*. Springer, New York, 1987.

[11] Daniel A Marcus. *Number fields*. Springer, New York, 1977.

[12] Arnold K Pizer. Ramanujan graphs and hecke operators. *Bulletin of the American Mathematical Society*, 23(1):127–137, 1990.

[13] Ren Schoof. Nonsingular plane cubic curves over finite fields. *Journal of combinatorial theory*, (Series A, 46(2)):183–211, 1987.

[14] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[15] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer Science & Business Media, 2013.

[16] P. Stevenhagen. Number rings. `http://websites.math.leidenuniv.nl/algebra/ant.pdf`, Oct. 2017.

[17] Andrew Sutherland. Isogeny volcanoes. *The Open Book Series*, 1(1):507–530, 2013.

[18] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.

[19] John Voight. Quaternion algebras. `https://math.dartmouth.edu/~jvoight/quat-book.pdf`, 2019. Version v.0.9.15.

[20] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. New York, 2008.

[21] William C Waterhouse. Abelian varieties over finite fields. In *Annales scientifiques de l'École Normale Supérieure*, volume 2, pages 521–560, 1969.

Appendix A. The discussion about the index problem in field with characteristic 0.

Consider two elliptic curves E_1, E_2 defined over a perfect field F with characteristic 0, then the endomorphism rings of them are $\mathbb{Z}$ or a imaginary quadratic order[14, Corollary III.9.4]. If $\mathrm{Hom}(E_1, E_2) \neq 0$ and $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}E_2) = 1$, then $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}E_1) = 1$ and $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}\beta_0$ where $\beta_0 \in \mathrm{Hom}(E_1, E_2)$. Hence for any isogeny $\beta : E_2 \to E_1$, we have

$$[\mathrm{End}(E_2) : \mathrm{Hom}(E_1, E_2)\beta] = (\frac{\deg\beta}{\deg\beta_0})^{\frac{1}{2}}\deg\beta_0.$$

If $\mathrm{Hom}(E_1, E_2) \neq 0$ and $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}E_2) = 2$, then $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}E_1) = 2$ and $\mathrm{End}(E_1)$ has the same endomorphism algebra as $\mathrm{End}(E_2)$. If E_1, E_2 are defined over some number field, then for any isogeny $\beta : E_2 \to E_1$, the index of $\mathrm{Hom}(E_1, E_2)\beta$ in $\mathrm{End}(E_2)$ has the same results with the ordinary case of elliptic curves defined over a finite field k. That is, if $\mathrm{End}(E_2) = \mathbb{Z} + \mathbb{Z}f\gamma$ and $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell_1^{e_1'} \cdots \ell_s^{e_s'}$ where $e_i' \in \mathbb{Z}_{\neq 0}$ for all i, then

$$[\mathrm{End}(E_2) : \mathrm{Hom}(E_1, E_2)\beta] = \prod_{i=1}^{s} \ell_i^{\rho(e_i')}\deg\beta.$$

For an elliptic curve E defined over $\mathbb{C}$, then there is a lattice L in the form $\mathbb{Z} + \mathbb{Z}\tau$ where τ lies in the upper half plane
$$\mathcal{H} = \{x + iy \in \mathbb{C} : y > 0\}, \text{ where } i^2 = -1,$$
such that $E \cong \mathbb{C}/L$. Given such two lattices $L_1 = \mathbb{Z} + \mathbb{Z}\tau_1$ and $L_2 = \mathbb{Z} + \mathbb{Z}\tau_2$, consider the isogenies from $\mathbb{C}/L_1$ to $\mathbb{C}/L_2$, according to [14, Theorem VI.5.3], it is equivalent to consider

$$\mathrm{Map}(L_1, L_2) = \{\alpha \in \mathbb{C} : \alpha L_1 \subseteq L_2\}.$$

Let K be an imaginary quadratic field, by some computations we have the following facts:

1) $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ has the endomorphism ring isomorphic to an order in K if and only if $\tau \in K$.

2) If $\tau_1 \in K$, then $\mathrm{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2) \neq 0$ if and only if $\tau_2 \in K$.

If τ_1 and τ_2 are not contained in any imaginary quadratic fields, and $\mathrm{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2) \neq 0$, then $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$. If $\tau_1 = a_0 + a_1\tau_2$ for some $a, b \in \mathbb{Q}$, then $\mathrm{Map}(L_1, L_2) = \mathbb{Z}m$ form some integer m. Otherwise, suppose $[\mathbb{Q}(\tau_2) : \mathbb{Q}] = n$, let τ_1 be in the form of $a_0 + a_1\tau_2 + \cdots + a_{n-1}\tau_2^{n-1}$ and the minimal polynomial of τ_2 be $b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n$ where $a_i, b_i \in \mathbb{Q}$ for all i, then $\mathrm{Map}(L_1, L_2) = \mathbb{Z}\beta$ where $\beta \notin \mathbb{Z}$ if and only if $a_{n-1} \neq 0$ and

$$\begin{pmatrix} a_2 & a_1 + a_{n-1}b_2 \\ a_3 & a_2 + a_{n-1}b_3 \\ \vdots & \vdots \\ a_{n-1} & a_{n-2} + a_{n-1}b_{n-1} \end{pmatrix}$$

has rank 1.

Appendix B. An application of Corollary 3.5.

Let K be an imaginary quadratic field, and $\mathbb{Z}[\gamma]$ be its algebraic integer ring. For simplicity, we assume $\gamma \neq \sqrt{-1}, \frac{1+\sqrt{-3}}{2}$. Arbitrarily given a conductor f, for any $\ell \mid f$, we can enumerate the number of invertible or non-invertible ideals of ℓ-power norms. We will recur to the Corollary 3.5. Since the endomorphism ring of $\mathbb{C}/(\mathbb{Z}[f\gamma])$ is $\mathbb{Z}[f\gamma]$, then after doing reduction by proper prime ideal , we can get an elliptic curve E defined over a finite field with endomorphism ring $\mathbb{Z}[f\gamma]$. Since distinct ideals of $\mathbb{Z}[f\gamma]$ correspond to distinct isogenies from E, to enumerate the number of invertible or non-invertible ideals of ℓ-power norms, it suffices to enumerate the number of the corresponding isogenies in the ℓ-volcano. Let D be the discriminant of K, $\mathrm{iG}(f, \ell^n)$ denote the number of invertible ideals of norm ℓ^n, and $\mathrm{niG}(f, \ell^n)$ denote the number of non-invertible ideals

of norm ℓ^n in the order with conductor f. Then we have the following results. For the invertible ideals, we have

$$\mathrm{iG}(f,\ell^n) = \begin{cases} 0 & \text{if } n \text{ is odd and } (i)\, 0 < n < 2v_\ell(f) \text{ or } (ii)(\frac{D}{\ell}) = -1; \\ \ell^{\frac{n}{2}} & \text{if } n \text{ is even and } 0 < n < 2v_\ell(f); \\ \ell^{v_\ell(f)-1}(\ell+1) & \text{if } n \geqslant 2v_\ell(f),\ n \text{ is even and } (\frac{D}{\ell}) = -1; \\ \ell^{v_\ell(f)} & \text{if } n \geqslant 2v_\ell(f) \text{ and } (\frac{D}{\ell}) = 0; \\ (n - 2v_\ell(f) + 1)\ell^{v_\ell(f)-1}(\ell-1) & \text{if } n \geqslant 2v_\ell(f) \text{ and } (\frac{D}{\ell}) = 1. \end{cases}$$

And for the non-invertible ideals, we have

$$\mathrm{niG}(f,\ell^n) = \sum_{1 \leqslant k \leqslant \min(n, v_\ell(f))} \mathrm{iG}\left(\frac{f}{\ell^k}, \ell^{n-k}\right),\ \text{ where } \mathrm{iG}(1,1) = 1.$$

Example 4. Consider the order $\mathbb{Z}[2^2\sqrt{-2}]$. We list the ideals and the numbers in the following table.

norm	invertible ideals		non-invertible ideals	
2		$\mathrm{iG}(2^2, 2) = 0$	$2\mathbb{Z} + 2^2\sqrt{-2}\mathbb{Z}$	$\mathrm{niG}(2^2, 2) = 1$
2^2	$2^2\mathbb{Z} + (2 + 2^2\sqrt{-2})\mathbb{Z}$ $2\mathbb{Z} + 2^3\sqrt{-2}\mathbb{Z}$	$\mathrm{iG}(2^2, 2^2) = 2$	$2^2\mathbb{Z} + 2^2\sqrt{-2}\mathbb{Z}$	$\mathrm{iG}(2,2) + \mathrm{iG}(1,1)$ $=0+1=1$
2^3		$\mathrm{iG}(2^2, 2^3) = 0$	$2^2\mathbb{Z} + 2^3\sqrt{-2}\mathbb{Z}$ $2^3\mathbb{Z} + (2^2 + 2^2\sqrt{-2})\mathbb{Z}$ $2^3\mathbb{Z} + 2^2\sqrt{-2}\mathbb{Z}$	$\mathrm{iG}(2,2^2) + \mathrm{iG}(1,2)$ $=2+1=3$
2^4	$2^2\mathbb{Z} + 2^4\sqrt{-2}\mathbb{Z}$ $2^3\mathbb{Z} + (2^2 + 2^3\sqrt{-2})\mathbb{Z}$ $2^4\mathbb{Z} + \mathbb{Z}(2^2 + 2^2\sqrt{-2})$ $2^4\mathbb{Z} + (2^23 + 2^2\sqrt{-2})\mathbb{Z}$	$\mathrm{iG}(2^2, 2^4) = 4$	$2^3\mathbb{Z} + 2^3\sqrt{-2}\mathbb{Z}$ $2^4\mathbb{Z} + 2^2\sqrt{-2}\mathbb{Z}$ $2^4\mathbb{Z} + (2^3 + 2^2\sqrt{-2})\mathbb{Z}$	$\mathrm{iG}(2,2^3) + \mathrm{iG}(1,2^2)$ $=2+1=3$
2^5	$2^5\mathbb{Z} + 2^2\sqrt{-2}\mathbb{Z}$ $2^5\mathbb{Z} + (2^3 + 2^2\sqrt{-2})\mathbb{Z}$ $2^5\mathbb{Z} + (2^4 + 2^2\sqrt{-2})\mathbb{Z}$ $2^5\mathbb{Z} + (2^33 + 2^2\sqrt{-2})\mathbb{Z}$	$\mathrm{iG}(2^2, 2^5) = 4$	$2^3\mathbb{Z} + 2^4\sqrt{-2}\mathbb{Z}$ $2^4\mathbb{Z} + (2^3 + 2^3\sqrt{-2})\mathbb{Z}$ $2^4\mathbb{Z} + 2^3\sqrt{-2}\mathbb{Z}$	$\mathrm{iG}(2,2^4) + \mathrm{iG}(1,2^3)$ $=2+1=3$