Finite Fields and Their Applications 61 (2020) 101600

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728

Songsong Li, Yi Ouyang, Zheng Xu *

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, China

ARTICLE INFO

Article history:
Received 1 May 2019
Received in revised form 26 July 2019
Accepted 3 October 2019
Available online 16 October 2019
Communicated by Neal Koblitz

MSC:
11G20
11G15
14G15
14H52
94A60

Keywords:
Supersingular elliptic curves over finite fields
Isogeny graph

ABSTRACT

We describe the neighborhood of the vertex $[E_0]$ (resp. $[E_{1728}]$) in the ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ of supersingular elliptic curves over the finite field $\mathbb{F}_{p^2}$ when $p > 3\ell^2$ (resp. $p > 4\ell^2$) with $E_0 : y^2 = x^3 + 1$ (resp. $E_{1728} : y^2 = x^3 + x$) supersingular.

* Corresponding author.
E-mail addresses: songsli@mail.ustc.edu.cn (S. Li), yiouyang@ustc.edu.cn (Y. Ouyang), xuzheng1@mail.ustc.edu.cn (Z. Xu).

https://doi.org/10.1016/j.ffa.2019.101600
1071-5797/

1. Introduction and main results

Elliptic curves over finite fields play an important role in cryptography. It is well-known that elliptic curves defined over finite fields can be classified into two types: ordinary and supersingular. If the elliptic curve E is ordinary, the endomorphism ring of E is an order of an imaginary quadratic field. If E is supersingular, the endomorphism ring of E is a maximal order of a quaternion algebra. Computing the endomorphism rings and computing the isogenies of elliptic curves over finite fields are interesting problems in number theory and also has applications in cryptography. Stolbunov [14] proposed a Diffie-Hellman type system based on the difficulty of computing isogenies between ordinary elliptic curves. Cryptosystems based on the hardness of computing the endomorphism rings and isogenies of supersingular elliptic curves were proposed in [9]. Thus, it is important to find an explicit isogeny between two elliptic curves.

The efficient method to find explicit isogenies between supersingular elliptic curves is to use the isogeny graph, which is a Ramanujan graph introduced in [4]. Childs, Jao and Soukharev gave an algorithm to compute ordinary elliptic curve isogenies in quantum subexponential time in [5]. For supersingular elliptic curves defined over $\mathbb{F}_p$, from [7,3], there is also a subexponential time algorithm to solve this problem.

However, for supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, it is hard to compute the endomorphism rings or isogenies of the curves. Let ℓ be a prime different from p. Here we recall the definition of the isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ over $\mathbb{F}_{p^2}$ by Adj et al. [1]. A vertex in the graph is an $\mathbb{F}_{p^2}$-isomorphism class $[E]$ of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. Let $[E_1] = [E_1']$, $[E_2] = [E_2']$ be two vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$, let $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_1' \to E_2'$ be two ℓ-degree $\mathbb{F}_{p^2}$-isogenies. We say that ϕ_1 and ϕ_2 are equivalent if there exist isomorphisms $\rho_1 : E_1 \to E_1'$ and $\rho_2 : E_2 \to E_2'$ such that $\phi_2\rho_1 = \rho_2\phi_1$. Then an edge in the graph is an equivalent class of ℓ-isogenies. If replacing the field of definition $\mathbb{F}_{p^2}$ of the curves and isogenies by the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, we get the definition of the isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$. Note that for E supersingular over $\mathbb{F}_{p^2}$, the trace of Frobenius $\pi = (x \mapsto x^{p^2})$ on the Tate module of E must be 0, $\pm p$ or $\pm 2p$. For $t \in \{0, \pm p, \pm 2p\}$, let $\mathcal{G}_\ell(\mathbb{F}_{p^2}, t)$ be the subgraph of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ consisting of vertices $[E]$ with Frobenius trace t and the adjacent edges.

Adj et al. [1] described clearly the subgraphs $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm p)$. However, more work needs to be done when $t = \pm 2p$. Adj et al. proved the following key result in [1, Theorem 6] and [1, page 10, line 24]:

$$\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p) \cong \mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p) \cong \mathcal{G}_\ell(\overline{\mathbb{F}}_p). \tag{1}$$

Hence to study the neighborhood of a vertex $[E]$ in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$, it suffices to study its neighborhood in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$. Then tools such as Deuring's Correspondence Theorem can be used.

For $p > 3$, there are two special supersingular elliptic curves over $\mathbb{F}_{p^2}$ with trace $-2p$:

$$E_0 : y^2 = x^3 + 1 \text{ when } p \equiv 2 \bmod 3$$

with j invariant 0 and

$$E_{1728} : y^2 = x^3 + x \text{ when } p \equiv 3 \bmod 4$$

with j-invariant 1728. Then Adj et al. [1, Theorems 10 and 12] and Ouyang-Xu [12] proved the following results about the loops on the vertices $[E_{1728}]$ and $[E_0]$ in the supersingular elliptic curves graph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$.

Theorem 1. *Suppose $\ell > 3$.*

(1) *If $p \equiv 3 \bmod 4$ and $p > 4\ell$, there are either 2 or 0 loops on $[E_{1728}]$ if $\ell \equiv 1 \bmod 4$ or 3 mod 4 respectively.*

(2) *If $p \equiv 2 \bmod 3$ and $p > 3\ell$, there are either 2 or 0 loops on $[E_0]$ if $\ell \equiv 1 \bmod 3$ or 2 mod 3 respectively.*

In this paper, we shall work on the neighborhood of the vertices $[E_0]$ and $[E_{1728}]$ in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$. Our main result is

Theorem 2. *Suppose $\ell > 3$.*

(1) *If $p \equiv 3 \bmod 4$ and $p > 4\ell^2$, there are $\frac{1}{2}\big(\ell - (-1)^{\frac{\ell-1}{2}}\big)$ vertices adjacent to $[E_{1728}]$ in the graph, each connecting $[E_{1728}]$ with 2 edges. Moreover, $1 + (\frac{\ell}{p})$ of the vertices are of j-invariants in $\mathbb{F}_p - \{1728\}$.*

(2) *If $p \equiv 2 \bmod 3$ and $p > 3\ell^2$, there are $\frac{1}{3}(\ell - (\frac{\ell}{3}))$ vertices adjacent to $[E_0]$ in the graph, each connecting $[E_0]$ with 3 edges. Moreover, $1 + (\frac{-p}{\ell})$ of the vertices are of j-invariants in $\mathbb{F}_p^*$.*

Remark. (1) It would be best if the bounds $4\ell^2$ and $3\ell^2$ can be improved to 4ℓ and 3ℓ, as is the case for the number of loops in Theorem 1. However, this speculation is actually false. For a fixed prime $\ell > 3$, let $P_1(\ell)$ (resp. $P_2(\ell)$) be the largest prime p such that the number of vertices adjacent to $[E_{1728}]$ (resp. $[E_0]$) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ is smaller than $\frac{1}{2}\big(\ell - (-1)^{\frac{\ell-1}{2}}\big)$ (resp. $\frac{1}{3}(\ell - (\frac{\ell}{3}))$), i.e., our main theorem fails for such a p. By numerical evidence presented in § 4, for $5 \leq \ell \leq 200$, most of the time $P_1(\ell)$ is the largest prime $\equiv 3 \bmod 4$ and smaller than $4\ell^2$, $P_2(47) = 6599$ is the largest prime $\equiv 2 \bmod 3$ and smaller than $3 \times 47^2 = 6627$. In this sense, our bounds are sharp.

(2) For $\ell = 2$ or 3, we shall describe the neighborhood of $[E_0]$ and $[E_{1728}]$ in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ for any prime $p > 3$ (such that either E_0 or E_{1728} is supersingular) in § 5.

As the j-invariants of elliptic curves adjacent to E_0 (resp. E_{1728}) are roots of the modular polynomial $\Phi_\ell(0, X)$ (resp. $\Phi_\ell(1728, X)$), our result has the following immediate consequences about their roots.

Theorem 3. *Suppose $\ell > 3$.*

(1) *If* $p \equiv 3 \bmod 4$ *and* $p > 4\ell^2$, *then if* $\ell \equiv 3 \bmod 4$,

$$\Phi_\ell(1728, X) = \prod_{i=1}^{(\ell+1)/2} (X - a_i)^2$$

with $1 + (\frac{\ell}{p})$ *of the roots* $a_i \in \mathbb{F}_p - \{1728\}$ *and the rest in* $\mathbb{F}_{P^2} - \mathbb{F}_p$; *if* $\ell \equiv 1 \bmod 4$,

$$\Phi_\ell(1728, X) = (X - 1728)^2 \prod_{i=1}^{(\ell-1)/2} (X - a_i)^2$$

with $1 + (\frac{\ell}{p})$ *of the roots* $a_i \in \mathbb{F}_p - \{1728\}$ *and the rest in* $\mathbb{F}_{p^2} - \mathbb{F}_p$.

(2) *If* $p \equiv 2 \bmod 3$ *and* $p > 3\ell^2$, *then if* $\ell \equiv 2 \bmod 3$,

$$\Phi_\ell(0, X) = \prod_{i=1}^{(\ell+1)/3} (X - a_i)^3$$

with $1 + (\frac{-p}{\ell})$ *of the roots* $a_i \in \mathbb{F}_p^*$ *and the rest in* $\mathbb{F}_{P^2} - \mathbb{F}_p$; *if* $\ell \equiv 1 \bmod 3$,

$$\Phi_\ell(0, X) = X^2 \prod_{i=1}^{(\ell-1)/3} (X - a_i)^3$$

with $1 + (\frac{-p}{\ell})$ *of the roots* $a_i \in \mathbb{F}_p^*$ *and the rest in* $\mathbb{F}_{p^2} - \mathbb{F}_p$.

2. Preliminaries

2.1. Elliptic curves over finite fields

We recall basic facts about elliptic curves over finite fields. The general reference is [13]. Let $\overline{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p$.

An elliptic curve E over the finite field $\mathbb{F}_q$ for q a power of $p > 3$ is defined by a Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$.

The trace of the Frobenius $\pi : (x, y) \mapsto (x^q, y^q)$ on the Tate module of E, which we also call the trace of E and denoted by $\mathrm{tr}(E)$, is the number $t = q + 1 - \#E(\mathbb{F}_q)$. The minimal polynomial of π is $x^2 - tx + q$ and Hasse's Theorem (see [13]) implies that $|t| \leq 2\sqrt{q}$.

The j-invariant of E, which determines the isomorphism class of E over $\overline{\mathbb{F}}_p$, is $j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2}$. The endomorphism ring $\mathrm{End}(E)$ of E is the set of all isogenies between E and itself. For E an elliptic curve over $\mathbb{F}_q$, $\mathrm{End}(E)$ is either an order of an imaginary quadratic field, in which case E is called ordinary; or a maximal order of a quaternion algebra, in which case E is called supersingular. It is well-known that E is ordinary

(resp. supersingular) if and only if $p \nmid t$ (resp. $p \mid t$). Moreover, a supersingular elliptic curve E over $\mathbb{F}_q$ always has j-invariant $j(E) \in \mathbb{F}_{p^2}$.

From now on, suppose E is supersingular. Since $j(E) \in \mathbb{F}_{p^2}$, we assume E is also defined over $\mathbb{F}_{p^2}$. Then $t = 0$, $\pm p$ or $\pm 2p$.

2.2. Quaternion algebra

A quaternion algebra over $\mathbb{Q}$ is of the form $H(a,b) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, where $i^2 = a$, $j^2 = b$ and $k = ij = -ji$. The canonical involution on $H(a,b)$ is the map sending $\alpha = a_1 + a_2 i + a_3 j + a_4 k \in H(a,b)$ to $\bar{\alpha} = a_1 - a_2 i - a_3 j - a_4 k$. The reduced trace of α is $\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2a_1$, and the reduced norm is $\mathrm{Nrd}(\alpha) = \alpha\bar{\alpha} = {a_1}^2 - a{a_2}^2 - b{a_3}^2 + ab{a_4}^2$. A subset Λ is a lattice in $H(a,b)$ if $\Lambda = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3 + \mathbb{Z}x_4$ and $\{x_1, x_2, x_3, x_4\}$ is a $\mathbb{Q}$-basis of $H(a,b)$.

The unique quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞ is $B_{p,\infty} = H(-1,-p)$.

2.3. Orders and ideals in $B_{p,\infty}$

An order $\mathcal{O}$ of $B_{p,\infty}$ is a subring of $B_{p,\infty}$ which is also a lattice, and is called a maximal order if it is not properly contained in any other order.

For $\mathcal{O}$ an order of $B_{p,\infty}$, let I be a left ideal of $\mathcal{O}$. The left order $\mathcal{O}_L(I)$ and right order $\mathcal{O}_R(I)$ of I are defined to be

$$\mathcal{O}_L(I) = \{x \in B_{p,\infty} \mid xI \subseteq I\}, \quad \mathcal{O}_R(I) = \{x \in B_{p,\infty} \mid Ix \subseteq I\}.$$

If $\mathcal{O}$ is a maximal order, then $\mathcal{O}_L(I) = \mathcal{O}$ and $\mathcal{O}_R(I) = \mathcal{O}'$ is also a maximal order, in which case we say that I connects $\mathcal{O}$ and $\mathcal{O}'$. Moreover, if $\mathcal{O}$ is maximal,

$$\mathcal{O}_R(I) = \mathcal{O} \iff I = \mathcal{O}x \text{ is principal.}$$

Define the reduced norm $\mathrm{Nrd}(I)$ of I by

$$\mathrm{Nrd}(I) = \gcd(\{\mathrm{Nrd}(\alpha) \mid \alpha \in I\}).$$

Lemma 4. *If $\mathcal{O}$ is a maximal order in $B_{p,\infty}$ and I is a left $\mathcal{O}$-ideal of reduced norm ℓ, then $\ell \in I$.*

Proof. Note that the abelian group $\mathcal{O}/I$ is of order $\mathrm{Nrd}(I)^2 = \ell^2$. Assume $\ell \notin I$. Then the image of 1 in $\mathcal{O}/I$ must be of order ℓ^2 and $\mathcal{O}/I \cong \mathbb{Z}/\ell^2\mathbb{Z}$ is a cyclic group. Let $\{1, a, b, c\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Let $t_a, t_b, t_c \in \mathbb{Z}$ such that $a - t_a$, $b - t_b$ and $c - t_c \in I$. We replace $\{a, b, c\}$ by $\{a - t_a, b - t_b, c - t_c\}$, then we get a $\mathbb{Z}$-basis $\{1, a, b, c\}$ of $\mathcal{O}$ such that $\{\ell^2, a, b, c\}$ is a $\mathbb{Z}$-basis of I. By computation, $\mathcal{O} \subseteq \mathcal{O}_R(I)$, since they are both maximal orders in $B_{p,\infty}$, $\mathcal{O}_L(I) = \mathcal{O} = \mathcal{O}_R(I)$. From [15, 16.6.14], $\bar{I}I = \ell\mathcal{O}_R(I)$, $I\bar{I} = \ell\mathcal{O}_L(I)$.

Thus $\bar{I}I = \ell\mathcal{O} \subseteq \mathcal{O}$, and $\bar{I} \subseteq \mathcal{O}_L(I) = \mathcal{O}$ by definition. Hence, $\ell\mathcal{O} = \bar{I}I \subseteq \mathcal{O}I \subseteq I$. We get a contradiction. □

Now assume $\mathcal{O}$ is a maximal order of $B_{p,\infty}$ containing a subring $\mathbb{Z}\langle i, j\rangle$ with $i^2 = -q$, $j^2 = -p$ and $ij = -ji$ such that $(q, p) = 1$. Let $K = \mathbb{Q}(i)$. Then its ring of integers $\mathcal{O}_K = \mathbb{Z}[i]$ if $q \equiv 1,\ 2 \bmod 4$ or $\mathbb{Z}[\frac{1+i}{2}]$ if $q \equiv 3 \bmod 4$. Let $R = \mathcal{O} \bigcap K$. Then $\mathbb{Z}[i] \subseteq R \subseteq \mathcal{O}_K$. Let $\epsilon = i$ if $R = \mathbb{Z}[i]$ or $\frac{1+i}{2}$ if $R = \mathcal{O}_K = \mathbb{Z}[\frac{1+i}{2}]$.

Let X_ℓ be the set of all left $\mathcal{O}$-ideals of reduced norm ℓ. Let $\hat{r} \in (R/\ell R)^\times$ and $r \in R$ a lifting of $\hat{r}$. Then for any $I \in X_\ell$, $\ell\mathcal{O} + Ir$, depending only on $\hat{r}$ regardless the lifting, is also in X_ℓ by using Lemma 4 and computing the reduced norm of elements in $\ell\mathcal{O} + Ir$. Kohel et al. [10] defined the action of $(R/\ell R)^\times$ on X_ℓ by

$$(R/\ell R)^\times \ \times \ X_\ell \ \to \ X_\ell; \ \ (\hat{r}, I) \ \mapsto \ \mathcal{O}\ell + Ir.$$

The following theorem was stated in [10] without a proof and we supply a proof here.

Theorem 5. *Assume $\mathcal{O}$, K and $R = \mathbb{Z}[\epsilon]$ as above. Assume the prime $\ell \nmid 2pq[\mathcal{O} : \mathbb{Z}\langle i, j\rangle]$.*

(1) If ℓ is inert in R, then $(R/\ell R)^\times$ acts transitively on X_ℓ with $(\mathbb{Z}/\ell\mathbb{Z})^\times$ the stabilizer.

(2) If ℓ splits in R, write $\ell R = \mathfrak{p}_1\mathfrak{p}_2$, then $\{\mathcal{O}\mathfrak{p}_1, \mathcal{O}\mathfrak{p}_2\} \subset X_\ell$, $(R/\ell R)^\times$ acts trivially on $\mathcal{O}\mathfrak{p}_1$ and $\mathcal{O}\mathfrak{p}_2$, and acts transitively on $X_\ell - \{\mathcal{O}\mathfrak{p}_1, \mathcal{O}\mathfrak{p}_2\}$ with $(\mathbb{Z}/\ell\mathbb{Z})^\times$ the stabilizer.

In both cases, for any $I \in X_\ell - \{\mathcal{O}\mathfrak{p}_1, \mathcal{O}\mathfrak{p}_2\}$ and for $a \in \mathbb{F}_\ell$, let $I_a := \ell\mathcal{O} + I(\tilde{a} + \epsilon)$ with $\tilde{a} \in \mathbb{Z}$ a lifting of a, then $X_\ell = \{I, I_a \mid a \in \mathbb{F}_\ell\}$.

Proof. As $\ell \nmid pq[\mathcal{O} : \mathbb{Z}\langle i, j\rangle]$, $\mathcal{O}/\ell\mathcal{O} = \mathbb{F}_\ell\langle i, j\rangle$ with $i^2 = -q$, $j^2 = -p$ and $ij = -ji = k$. From [8], there is a ring isomorphism $\theta :\ \mathcal{O}/\ell\mathcal{O} \to M_2(\mathbb{F}_\ell)$ given by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i \mapsto \begin{pmatrix} 0 & -q \\ 1 & 0 \end{pmatrix},\ j \mapsto \begin{pmatrix} u & qv \\ v & -u \end{pmatrix}$$

where $(u,\ v)$ is a solution of $u^2 + qv^2 = -p$ in $\mathbb{F}_\ell$ (note that this equation is always solvable in $\mathbb{F}_\ell$).

From [2, Theorem 6 in §13], since $M_2(\mathbb{F}_\ell)$ is semi-simple and the only simple left $M_2(\mathbb{F}_\ell)$-module is 2-dimensional over $\mathbb{F}_\ell$, every nonzero proper left ideal must be a simple left $M_2(\mathbb{F}_\ell)$-module and is generated by just one element $M \neq 0$. For M is not invertible, $\mathrm{rank}(M) = 1$. Since $M_2(\mathbb{F}_\ell)M = M_2(\mathbb{F}_\ell)PM$ for any $P \in \mathrm{GL}_2(\mathbb{F}_\ell)$, we may assume that $M = \omega := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ or $\omega_a := \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix}$ for some $a \in \mathbb{F}_\ell$. Moreover, ω and ω_a generate different left ideals of $M_2(\mathbb{F}_\ell)$. Thus the set of all non-zero proper left ideals of $M_2(\mathbb{F}_\ell)$ is the set

$$\overline{X_\ell} := \{M_2(\mathbb{F}_\ell)\omega, M_2(\mathbb{F}_\ell)\omega_a \mid a \in \mathbb{F}_\ell\}.$$

Consequently, by the isomorphism θ, $\mathcal{O}/\ell\mathcal{O}$ has $\ell + 1$ non-zero proper left ideals, all of them are principal.

Under the canonical homomorphism $\mathcal{O} \to \mathcal{O}/\ell\mathcal{O}$ and θ, from Lemma 4, the set X_ℓ maps bijectively to the set of nonzero left ideals of $\mathcal{O}/\ell\mathcal{O}$ and hence to $\overline{X_\ell}$. Moreover, the action of $(R/\ell R)^\times$ on X_ℓ corresponds to the right multiplication of $(R/\ell R)^\times$ on the set of nonzero left ideals of $\mathcal{O}/\ell\mathcal{O}$, and to the right multiplication action of $\theta((R/\ell R)^\times)$ on $\overline{X_\ell}$.

Every element in $\theta((R/\ell R)^\times)$ is of the form $\begin{pmatrix} x & -qy \\ y & x \end{pmatrix}$ with $x^2 + qy^2 \neq 0$. If $a_0 \in \mathbb{F}_\ell$ satisfying $a_0^2 + q = 0$, then $x + a_0 y \neq 0$ and

$$\omega_{a_0} \begin{pmatrix} x & -qy \\ y & x \end{pmatrix} = \begin{pmatrix} x + a_0 y & a_0(x + a_0 y) \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{F}_\ell)\omega_{a_0}.$$

If $a \in \mathbb{F}_\ell$ satisfying $a^2 + q \neq 0$, then for any b such that $b^2 + q \neq 0$,

$$\omega_a \begin{pmatrix} \frac{q+ab}{q+a^2} & -q\frac{a-b}{q+a^2} \\ \frac{a-b}{q+a^2} & \frac{q+ab}{q+a^2} \end{pmatrix} = \omega_b, \tag{2}$$

and

$$\omega_a \begin{pmatrix} \frac{a}{q+a^2} & q\frac{1}{q+a^2} \\ -\frac{1}{q+a^2} & \frac{a}{q+a^2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{F}_\ell)\omega. \tag{3}$$

Since $\ell \nmid 2q$, ℓ is prime to the conductor of R and $R\ell$ is the product of at most two prime R-ideals.

If ℓ is inert in R, there is no $a_0 \in \mathbb{F}_\ell$ such that ${a_0}^2 + q = 0$, thus the action of $\theta((R/\ell R)^\times)$ on $\overline{X_\ell}$ is transitive by (2) and (3). In this case, $\{1, a+\epsilon \mid 0 \leq a \leq \ell - 1\}$ is a coset representative of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ in $(R/\ell R)^\times$, hence $X_\ell = \{I, I_a \mid a \in \mathbb{F}_\ell\}$ where I is any element in X_ℓ.

If $\ell R = \mathfrak{p}_1\mathfrak{p}_2$ splits in R, then $\mathfrak{p}_1 = (\ell, a+\epsilon)$ and $\mathfrak{p}_2 = \bar{\mathfrak{p}}_1 = (\ell, a+\bar{\epsilon})$ for some $a \in \mathbb{Z}$ such that $N(a+\epsilon) = \mathrm{Nrd}(a+\epsilon) = 0 \in \mathbb{F}_\ell$, this implies that $\mathcal{O}\mathfrak{p}_1 = \ell\mathcal{O} + \mathcal{O}(a+\epsilon)$ and $\mathcal{O}\mathfrak{p}_2 = \ell\mathcal{O} + \mathcal{O}(a+\bar{\epsilon})$ are in X_ℓ. This also implies that there exists some $a_0 \in \mathbb{F}_\ell$ such that ${a_0}^2 + q = 0$. Thus $\theta((R/\ell R)^\times)$ has one orbit of length $\ell - 1$ and two fixed points ω_{a_0}, ω_{-a_0}. In this case, $\{1, b+\epsilon \mid b \in \mathbb{F}_\ell, N(b+\epsilon) \neq 0\}$ is a coset representative of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ in $(R/\ell R)^\times$. For $I = \mathcal{O}\mathfrak{p}_1 = \ell\mathcal{O} + \mathcal{O}(a+\epsilon)$ or $\mathcal{O}\mathfrak{p}_2$, $\ell\mathcal{O} + Ir = \ell\mathcal{O} + rI \subseteq I$, they must be equal since both are left $\mathcal{O}$-ideals of reduced norm ℓ. Thus for any $I \in X_\ell - \{\mathcal{O}\mathfrak{p}_1, \mathcal{O}\mathfrak{p}_2\}$, we still have $X_\ell = \{I, I_a \mid a \in \mathbb{F}_\ell\}$. □

Remark. For any $I \in X_\ell$, from the proof of Theorem 5, we have $I = \mathcal{O}\ell + \mathcal{O}\alpha$ for some $\alpha \in \mathcal{O}$.

From now on, by abuse of notation, we identify $\mathbb{F}_\ell$ with the set $\{0, \cdots, \ell - 1\}$ and $\tilde{a}$ with a in the definition of I_a.

2.4. Supersingular elliptic curves and $B_{p,\infty}$

Suppose E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$, then $\mathrm{End}(E) = \mathcal{O}$ is a maximal order of a quaternion algebra $B_{p,\infty}$. For I a left integral ideal of $\mathcal{O}$, let $E[I] = \{P \in E \mid \alpha(P) = O \text{ for every } \alpha \in I\}$, then the isogeny

$$\phi_I : E \to E_I = E/E[I]$$

has $\ker \phi_I = E[I]$ and $\deg(\phi_I) = \mathrm{Nrd}(I)$ the reduced norm of I. On the other hand, if $\phi : E \to E'$ is an isogeny of degree n, then $\ker \phi$ is of order n and $I_\phi = \{\alpha \in \mathcal{O} \mid \alpha(P) = O \text{ for all } P \in \ker \phi\}$ is a left $\mathcal{O}$-ideal of reduced norm n. Deuring's Correspondence Theorem (see Voight [15, chapter 42] or [6]) is the following theorem:

Theorem 6. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ and $\mathrm{End}(E) = \mathcal{O}$. Then $\mathcal{O}$ is a maximal order of $B_{p,\infty}$.*

(1) *There is a 1-to-1 correspondence between left ideals I of $\mathcal{O}$ of reduced norm n and equivalent classes of isogenies $\phi : E \to E'$ of degree n given by $I \mapsto [\phi_I]$ and $[\phi] \mapsto I_\phi$.*

(2) *If $\phi : E \to E'$ and I are corresponding to each other, then $\mathrm{End}(E') \cong \mathcal{O}_R(I)$ is the right order of I in $B_{p,\infty}$. In particular, $\phi \in \mathrm{End}(E)$ if and only if $I = I_\phi = \mathcal{O}\phi$ is principal.*

(3) *Suppose that $\phi_1 : E \to E_1$, $\phi_2 : E \to E_2$ are two isogenies corresponding to the left ideals $I_1, I_2 \subseteq \mathcal{O}$. Then E_1 and E_2 are in the same isomorphism class if and only if $I_1 = I_2 x$ for some $x \in B_{p,\infty}$, i.e. I_1 and I_2 are in the same left ideal class.*

3. Proof of main theorem

By the isomorphism $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p) \cong \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, to study the neighborhoods of $[E_0]$ and $[E_{1728}]$ in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$, it suffices to study the neighborhoods of $[E_0]$ and $[E_{1728}]$ in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

From [11], in the cases when E_0 or E_{1728} is supersingular ($p \equiv 2 \bmod 3$ for E_0 and $p \equiv 3 \bmod 4$ for E_{1728}), then

$$\mathrm{End}(E_0) = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}j + \mathbb{Z}\frac{3+i+3j+k}{6} \tag{4}$$

where $i^2 = -3$, $j^2 = -p$ and $ij = -ji = k$; and

$$\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} \tag{5}$$

where $i^2 = -1$, $j^2 = -p$ and $ij = -ji = k$.

We shall apply Theorem 5 in both cases. Let I be a left $\mathrm{End}(E_0)$ or $\mathrm{End}(E_{1728})$ ideal of reduced norm ℓ not above ℓ, then the set X_ℓ of all left ideals of reduced norm ℓ is $\{I,\ I_a \mid a \in \mathbb{F}_\ell\}$ by Theorem 5. The strategy of our proof is to find all left ideal classes

of X_ℓ and the size of each ideal class. Then applying Deuring's Theorem, we obtain information of vertices and edges in the neighborhoods of $[E_0]$ and $[E_{1728}]$.

We need the following easy lemma:

Lemma 7. *Let N be a $\mathbb{Z}$-module and M a submodule of N. Then for coprime integers n and m, $mM + nN = M + nN$.*

3.1. Neighborhood of $[E_{1728}]$

This subsection is devoted to the proof of Theorem 2(1).

Write $\mathcal{O} = \mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2}$ where $i^2 = -1$, $j^2 = -p$ and $ij = -ji = k$. In this case $R = \mathcal{O} \cap \mathbb{Q}(i) = \mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(i)}$ is a principal ideal domain and its unit group is $\{\pm 1, \pm i\}$.

Lemma 8. *Suppose $\ell \equiv 1 \bmod 4$.*

(1) *ℓ splits completely in $\mathbb{Z}[i]$, $\ell\mathbb{Z}[i] = (m+ni)\mathbb{Z}[i]\cdot(m-ni)\mathbb{Z}[i]$ with $(m,n) \in \mathbb{Z}^2$ being any solution of $X^2+Y^2 = \ell$. The solution set of $X^2+Y^2 = \ell$ is $\{(\pm m, \pm n), (\pm n, \pm m)\}$.*

(2) *The set of pairs $(x,y) \in \mathbb{Z}^2$ satisfying $\ell \nmid x$ and $X^2 + Y^2 = \ell^2$ is $\{(\pm(m^2 - n^2), \pm 2mn), (\pm 2mn, \pm(m^2 - n^2))\}$.*

(3) *The two left $\mathcal{O}$-ideals $\mathcal{O}(m+ni)$ and $\mathcal{O}(m-ni)$ are of reduced norm ℓ. Moreover, for J any left $\mathcal{O}$-ideal of reduced norm ℓ, let $b = m/n \in \mathbb{F}_\ell$, then $b^2 = -1$, $J_b = \ell\mathcal{O} + J(\tilde{b} + i) = \ell\mathcal{O} + J(m + ni) = \mathcal{O}(m + ni)$ and $J_{-b} = \mathcal{O}(m - ni)$.*

Proof. All except the last part of (3) are classical results in number theory. That $b^2 = -1$ is clear. By Lemma 7, $J_b = \ell\mathcal{O} + J(m + ni) \subseteq \mathcal{O}(m + ni)$, but both of them are left $\mathcal{O}$-ideals of reduced norm ℓ, we have $J_b = \mathcal{O}(m + ni)$. Similarly $J_{-b} = \mathcal{O}(m - ni)$. □

Lemma 9. *Suppose $p > 4\ell^2$.*

(1) *If $\mu \in \ell^{-1}\mathcal{O}$, $\mathrm{Nrd}(\mu) = 1$ and $\mu \notin \{\pm 1, \pm i\}$, then $\ell \equiv 1 \bmod 4$ and $\mu = \ell^{-1}(x+yi)$ where $(x,y) \in \mathbb{Z}^2$ satisfies $\ell \nmid x$ and $X^2 + Y^2 = \ell^2$.*

(2) *If $s \in \ell^{-1}\mathcal{O}$, $s^2 = -p$ and $s \notin \{\pm j, \pm k\}$, then $\ell \equiv 1 \bmod 4$, and $s = \ell^{-1}(xj + yk)$ where $(x,y) \in \mathbb{Z}^2$ satisfies $\ell \nmid x$ and $X^2 + Y^2 = \ell^2$.*

Proof. (1) Write

$$\mu = \frac{1}{\ell}\Big(A + Bi + C\frac{1+j}{2} + D\frac{i+k}{2}\Big), \quad (A, B, C, D \in \mathbb{Z}).$$

By the fact $\mathrm{Nrd}(\mu) = 1$, then

$$\Big(A + \frac{C}{2}\Big)^2 + \Big(B + \frac{D}{2}\Big)^2 + \frac{p(C^2 + D^2)}{4} = \ell^2.$$

If $p > 4\ell^2$, then $C = D = 0$ and hence $\mu = \frac{A+Bi}{\ell}$ and $A^2 + B^2 = \ell^2$. If $\ell \mid A$, then $\ell \mid B$ and $\mu \in \{\pm 1, \pm i\}$. If $\ell \nmid A$, then $(B/A)^2 = -1 \in \mathbb{F}_\ell$ and $\ell \equiv 1 \bmod 4$.

(2) Write $s = \ell^{-1}(a + bi + c\frac{1+j}{2} + d\frac{i+k}{2})$. Then $s^2 = -p \in \mathbb{Q}$ implies $a + \frac{c}{2} = 0$ and $c \in 2\mathbb{Z}$. Moreover,

$$\ell^2 p = -\ell^2 s^2 = \mathrm{Nrd}(\ell s) = \left(b + \frac{d}{2}\right)^2 + \frac{p}{4}(c^2 + d^2)$$

implies $p \mid 2b+d$. If $2b+d \neq 0$, then $(b+\frac{d}{2})^2 \geq \frac{p^2}{4} > p\ell^2$ since $p > 4\ell^2$, impossible. Hence $b+\frac{d}{2} = 0$ and $d \in 2\mathbb{Z}$. Hence $s \in \ell^{-1}\mathcal{O}$ with $s^2 = -p$ must have the form $s = \ell^{-1}(xj+yk)$ with $x, y \in \mathbb{Z}$ and $x^2+y^2 = \ell^2$. If $\ell \mid x$, then $\ell \mid y$. It means $s = Xj+Yk$ $(X, Y \in \mathbb{Z})$, for $\mathrm{Nrd}(Xj+Yk) = (X^2+Y^2)p$, then the square roots of $-p$ in $\mathbb{Z}[j,k]$ are $\{\pm j, \pm k\}$. And we get $s \in \{\pm j, \pm k\}$. Otherwise we again have $(y/x)^2 = -1 \in \mathbb{F}_\ell$ and $\ell \equiv 1 \bmod 4$. □

Proof of Theorem 2(1). Let $\ell \neq p$ be a prime. If $\ell \equiv 1 \bmod 4$, let $(m, n) \in \mathbb{Z}^2$ be any solution of $x^2 + y^2 = \ell$ and $b = mn^{-1} \in \mathbb{F}_\ell$ in this case, then $b^2 = -1$.

Let I be a left $\mathcal{O}$-ideal of reduced norm ℓ different from $\mathcal{O}(m \pm ni)$ if $\ell \equiv 1 \bmod 4$. By Theorem 5, the set of the $\ell + 1$ left $\mathcal{O}$-ideals of reduced norm ℓ is

$$X_\ell = \{I,\ I_a = \ell\mathcal{O} + I(a+i) \mid a \in \mathbb{F}_\ell = \{0, \cdots, \ell-1\}\}.$$

If $\ell \equiv 1 \bmod 4$, by Lemma 8, $I_b = \mathcal{O}(m+ni)$ and $I_{-b} = \mathcal{O}(m-ni)$.

We claim that $Ii = I_0$, $I_0 i = I$ and $I_a i = I_{-a^{-1}}$ if $a \neq 0$. Indeed, from Lemma 4, $\ell \in I$. Then $\ell i \in I$ and $\ell = -\ell ii \in Ii$, hence $I_0 = Ii + \ell\mathcal{O} = Ii$ and $I = I_0 i$. For $a \neq 0$ in $\mathbb{F}_\ell$, $i \in \mathcal{O}$ then $\ell\mathcal{O}i \subseteq \ell\mathcal{O}$, and $I_a i$ is left-$\mathcal{O}$ ideal, $\ell\mathcal{O} \subseteq I_a i$. It implies $I_a i = \ell\mathcal{O}i + I(-1+ai) = \ell\mathcal{O} + \ell\mathcal{O}i + I(-a^{-1}+i) = \ell\mathcal{O} + I(-a^{-1}+i) = I_{-a^{-1}}$, where the second identity is by Lemma 7.

To summarize, we divide X_ℓ into $\frac{\ell+1}{2}$ subsets, each consisting of 2 elements in the same ideal class: $\{I, I_0\}$, $\{I_a, I_{-a^{-1}}\}$ $(a^2 \neq 0, -1)$ and $\{I_b, I_{-b}\}$ for $b^2 = -1$. We show that any two left ideals in different subsets are not in the same ideal class by contradiction.

Suppose I and J are from different subsets of X_ℓ and $I = J\mu$ for some $\mu \in B_{p,\infty}$, then $\mu \notin \{\pm 1, \pm i\}$ and $\mathrm{Nrd}(\mu) = 1$. Since $\ell \in J$, $\ell\mu \in I \subseteq \mathcal{O}$ and $\mu \in \ell^{-1}\mathcal{O}$. By Lemma 9(1), we have $\ell \equiv 1 \bmod 4$, $\mu = \frac{A+Bi}{\ell}$, $A^2 + B^2 = \ell^2$ and $\ell \nmid A$. This means that $A + Bi = u(m \pm ni)^2$ for $u \in \{\pm 1, \pm i\}$, and thus $\gcd(A+Bi, \ell)$ in $\mathbb{Z}[i]$ is $u(m \pm ni)$. In particular $I_{\pm b} = \mathcal{O}(m+ni) \subseteq I$ and hence $I_{\pm b} = I$ as both are of the same reduced norm. Switch the role of I and J, we get $J = I_{\pm b}$. Hence both I and J are in the same subset $\{I_b, I_{-b}\}$, impossible. By Deuring's Theorem (Theorem 6), and from Theorem 1, when $\ell \equiv 3 \bmod 4$, none of the subsets consist of ideals corresponding to endomorphisms. This completes the proof of the first part of Theorem 2(1).

For the second part, let E be a supersingular elliptic curve defined over $\mathbb{F}_p$ such that E_{1728} connects to E via a left $\mathcal{O}$-ideal of reduced norm ℓ. By [7, Proposition 2.4], a supersingular elliptic curve is defined over $\mathbb{F}_p$ if and only if $\mathbb{Z}[\sqrt{-p}]$ is contained in its endomorphism ring. Then $\mathrm{End}(E) = \mathcal{O}_R(I) \subseteq \ell^{-1}\mathcal{O}$ has an element s such that $s^2 = -p$. By Lemma 9(2), we know either $s \in \{\pm j, \pm k\}$ or in the case $\ell \equiv 1 \bmod 4$, $\ell s = xj + yk$, $(x, y) \in \mathbb{Z}^2$ such that $\ell \nmid x$ and $x^2 + y^2 = \ell^2$.

Let $\hat{\mathcal{O}} = \mathcal{O}/\ell\mathcal{O}$. Then $\hat{\mathcal{O}}$ is a quaternion algebra over $\mathbb{F}_\ell$. We can identify $\hat{\mathcal{O}}$ with $M_2(\mathbb{F}_\ell)$ via the isomorphism θ in Theorem 5 with $q = 1$. Moreover, the set $\overline{X_\ell}$ defined in Theorem 5 corresponds to X_ℓ bijectively. Let I_a be the left $\mathcal{O}$-ideal of reduced norm ℓ corresponding to $\hat{I}_a = M_2(\mathbb{F}_\ell)\omega_a$ in $\overline{X}_\ell$. For $s \in \mathcal{O}$, let $\hat{s}$ be the image of s in $M_2(\mathbb{F}_\ell)$. By abuse of notation, write i, j, k for $\hat{i}$, $\hat{j}$ and $\hat{k}$.

If $(\frac{-p}{\ell}) = 1$, let $t \in \mathbb{F}_\ell$ such that $t^2 = -p$ and let $(u, v) = (t, 0)$. In this case, $I_\infty = \mathcal{O}\ell + \mathcal{O}(-t + j)$, $I_a = \mathcal{O}\ell + \mathcal{O}(-t + j)(a + i)$. Then one can easily check that $\hat{I}_\infty j \subset \hat{I}_\infty$, $\hat{I}_0 j \subset \hat{I}_0$ and $\hat{I}_a j \nsubseteq \hat{I}_a$ for all other a, this means $j \in \mathcal{O}_R(I_\infty)$, $j \in \mathcal{O}_R(I_0)$ but $j \notin \mathcal{O}_R(I_a)$ for other a. Similarly $k \in \mathcal{O}_R(I_{\pm 1})$ and $k \notin \mathcal{O}_R(I_a)$ for other a. Now if $\ell \equiv 1 \bmod 4$ and (x, y) any solution that $x^2 + y^2 = \ell^2$ and $\ell \nmid x$, then one can check $\hat{I}_a(\hat{x}j + \hat{y}k) \neq 0$ if $a^2 \neq -1$, hence $\mathcal{O}(xj + yk) \nsubseteq \ell\mathcal{O}$ and $\ell^{-1}(xj + yk) \notin O_R(I_a)$ if $a^2 \neq -1$. If $a^2 = -1$, then $I_a = \mathcal{O}(m + ni)$ or $I_a = (m - ni)$ for $m^2 + n^2 = \ell$, corresponding to the loops. In conclusion, there are two vertices defined over $\mathbb{F}_p$ adjacent to $[E_{1728}]$, one corresponding to the ideal class $[I_\infty] = [I_0]$ and the other corresponding to the ideal class $[I_1] = [I_{-1}]$.

If $(\frac{-p}{\ell}) = -1$, then $uv \neq 0$ for any solution (u, v) of $X^2 + Y^2 = -p$. It is easy to check $\omega j \notin \hat{I}_\infty$. For $a \in \mathbb{F}_\ell$, $\omega_a j \in \hat{I}_a$ implies that $2au = (1 - a^2)v$. From $uv \neq 0$, then $a \neq 0, \pm 1$ and $v = \frac{2a}{1-a^2}u$. Hence $-p = \frac{(1+a^2)^2}{(1-a^2)^2}u^2$, impossible. This means $j \notin I_a$ for all $a \in \mathbb{F}_\ell \cup \{\infty\}$. Similarly $k \notin I_a$ for all $a \in \mathbb{F}_\ell \cup \{\infty\}$. Also, if $x, y \neq 0$ such that $\omega_a(x + yi)j = 0$, by computation, $a^2 + 1 = 0$, which corresponds to the loops. In conclusion, there is no vertex defined over $\mathbb{F}_p$ other than $[E_{1728}]$. □

3.2. Neighborhood of $[E_0]$

This subsection is devoted to the proof of Theorem 2(2).

Write $\mathcal{O} = \mathrm{End}(E_0) = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{i+k}{3} + \mathbb{Z}\frac{j+k}{2}$ where $i^2 = -3$, $j^2 = -p$ and $ij = -ji = k$. Write $\epsilon = \frac{1+i}{2}$. Then $\mathbb{Z}[\epsilon] = \mathcal{O} \cap \mathbb{Q}(i)$, as the ring of integers of $\mathbb{Q}(i)$, is a principal ideal domain and its unit group is $\{\pm 1, \pm\epsilon, \pm\bar{\epsilon}\}$.

Lemma 10. *Suppose* $\ell \equiv 1 \bmod 3$.

(1) ℓ *splits completely in* $\mathbb{Z}[\epsilon]$, $\ell\mathbb{Z}[\epsilon] = (m + n\epsilon)\mathbb{Z}[\epsilon] \cdot (m + n\bar{\epsilon})\mathbb{Z}[\epsilon]$ *with* $(m, n) \in \mathbb{Z}^2$ *being any solution of* $X^2 + XY + Y^2 = \ell$. *The solution set of* $X^2 + XY + Y^2 = \ell$ *is* $\{\pm(m, n), \pm(n, m), \pm(m + n, -n), \pm(m + n, -m), \pm(-n, m + n), \pm(-m, m + n)\}$.

(2) *The set of pairs* $(x, y) \in \mathbb{Z}^2$ *satisfying* $\ell \nmid x$ *and* $X^2 + XY + Y^2 = \ell^2$ *is* $\{\pm((m^2 - n^2), n^2 + 2mn), (\pm(n^2 - m^2), \pm(m^2 + 2mn)), \pm((m^2 + 2mn), -(n^2 + 2mn)), \pm((n^2 + 2mn), -(m^2 + 2mn)), \pm((m^2 + 2mn), n^2 - m^2), \pm((n^2 + 2mn), m^2 - n^2)\}$.

(3) *The two left* $\mathcal{O}$*-ideals* $\mathcal{O}(m + n\epsilon)$ *and* $\mathcal{O}(m + n\bar{\epsilon})$ *are of reduced norm* ℓ. *Moreover, for* J *any left* $\mathcal{O}$*-ideal of reduced norm* ℓ, *let* $b = m/n \in \mathbb{F}_\ell$, *then* $b^2 + b + 1 = 0$, $J_b = \ell\mathcal{O} + J(\tilde{b} + \epsilon) = \ell\mathcal{O} + J(m + n\epsilon) = \mathcal{O}(m + n\epsilon)$ *and* $J_{b^2} = \mathcal{O}(m + n\bar{\epsilon})$.

Proof. Similar to the proof of Lemma 8. □

Lemma 11. *Suppose $p > 3\ell^2$.*

(1) *If $\mu \in \ell^{-1}\mathcal{O}$, $\mathrm{Nrd}(\mu) = 1$ and $\mu \notin \{\pm 1, \pm\epsilon, \pm\bar{\epsilon}\}$, then $\ell \equiv 1 \bmod 3$ and $\mu = \ell^{-1}(x + y\epsilon)$ where $(x, y) \in \mathbb{Z}^2$ satisfies $\ell \nmid x$ and $X^2 + XY + Y^2 = \ell^2$.*

(2) *If $s \in \ell^{-1}\mathcal{O}$, $s^2 = -p$ and $s \notin \{\pm j, \pm\epsilon j, \pm\bar{\epsilon} j\}$, then $\ell \equiv 1 \bmod 3$, and $s = \ell^{-1}(x + y\epsilon)j$ where $(x, y) \in \mathbb{Z}^2$ satisfies $\ell \nmid x$ and $X^2 + XY + Y^2 = \ell^2$.*

Proof. (1) Write

$$\mu = \frac{1}{\ell}\Big(A + B\frac{1+i}{2} + C\frac{i+k}{3} + D\frac{j+k}{2}\Big), \quad (A, B, C, D \in \mathbb{Z}).$$

By the fact $\mathrm{Nrd}(\mu) = 1$, then

$$\Big(A + \frac{B}{2}\Big)^2 + 3\Big(\frac{B}{2} + \frac{C}{3}\Big)^2 + \frac{p}{3}(C^2 + 3CD + 3D^2) = \ell^2.$$

If $p > 3\ell^2$, then $C = D = 0$ and hence $\mu = \frac{A+B\frac{1+i}{2}}{\ell}$ and $A^2 + AB + B^2 = \ell^2$. If $\ell \mid A$, then $\ell \mid B$ and $\mu \in \{\pm 1, \pm\frac{1+i}{2}, \pm\frac{1-i}{2}\}$. If $\ell \nmid A$, then $(B/A)^2 + (B/A) + 1 = 0 \in \mathbb{F}_\ell$ and $\ell \equiv 1 \bmod 3$.

(2) Write $s = \ell^{-1}(a + b\frac{1+i}{2} + c\frac{i+k}{3} + d\frac{j+k}{2})$. Then $s^2 = -p \in \mathbb{Q}$ implies $a + \frac{b}{2} = 0$ and $b \in 2\mathbb{Z}$. Moreover,

$$\ell^2 p = -\ell^2 s^2 = \mathrm{Nrd}(\ell s) = 3\left(\frac{b}{2} + \frac{c}{3}\right)^2 + \frac{p}{3}(c^2 + 3cd + 3d^2)$$

implies $p \mid \frac{3}{2}b + c$. If $\frac{3}{2}b + c \neq 0$, then $3(\frac{b}{2} + \frac{c}{3})^2 \geq \frac{p^2}{3} > p\ell^2$ since $p > 3\ell^2$, impossible. Hence $\frac{3}{2}b + c = 0$ and $c \in 3\mathbb{Z}$. Hence $s \in \ell^{-1}\mathcal{O}$ with $s^2 = -p$ must have the form $s = \ell^{-1}(x + y\frac{1+i}{2})j$ with $x, y \in \mathbb{Z}$ and $x^2 + xy + y^2 = \ell^2$. If $\ell \mid x$, then $\ell \mid y$. It means $s = (X + Y\frac{1+i}{2})j$ $(X, Y \in \mathbb{Z})$, for $\mathrm{Nrd}((X + Y\frac{1+i}{2})j) = (X^2 + XY + Y^2)p$, then the square roots of $-p$ in $\mathbb{Z}[j, \frac{1+i}{2}j]$ are $\{\pm j, \pm\frac{1+i}{2}j, \pm\frac{1-i}{2}j\}$. And we get $s \in \{\pm j, \pm\frac{1+i}{2}j, \pm\frac{1-i}{2}j\}$. Otherwise we again have $(y/x)^2 + (y/x) + 1 = 0 \in \mathbb{F}_\ell$ and $\ell \equiv 1 \bmod 3$. □

Proof of Theorem 2(2). Let $\ell \neq p$ be a prime. If $\ell \equiv 1 \bmod 3$, let $(m, n) \in \mathbb{Z}^2$ be any solution of $x^2 + xy + y^2 = \ell$ and $b = mn^{-1} \in \mathbb{F}_\ell$ in this case, then $b^2 + b + 1 = 0$.

Let I be a left $\mathcal{O}$-ideal of reduced norm ℓ different from $\mathcal{O}(m + n\epsilon)$ and $\mathcal{O}(m + n\bar{\epsilon})$ if $\ell \equiv 1 \bmod 3$. By Theorem 5, the set of the $\ell + 1$ left $\mathcal{O}$-ideals of reduced norm ℓ is

$$X_\ell = \{I,\ I_a = \ell\mathcal{O} + I(a + \frac{1+i}{2}) \mid a \in \mathbb{F}_\ell = \{0, \cdots, \ell - 1\}\}.$$

If $\ell \equiv 1 \bmod 3$, by Lemma 10, $I_b = \mathcal{O}(m + n\epsilon)$ and $I_{b^2} = \mathcal{O}(m + n\bar{\epsilon})$.

We claim that $I\epsilon = I_0$, $I\bar{\epsilon} = I_{-1}$ and $I_a\epsilon = I_{-(a+1)^{-1}}$, $I_a\bar{\epsilon} = I_{-a^{-1}(a+1)}$ if $a \neq 0, -1$. Indeed, from Lemma 4, $\ell \in I$. Then $\ell, \ell\bar{\epsilon} \in I$ and $\ell = \ell\bar{\epsilon}\epsilon \in I\epsilon$, hence $I_0 = I\epsilon + \ell\mathcal{O} = I\epsilon$. Similarly, $I\bar{\epsilon} = I_{-1}$. For $a \neq 0, -1$ in $\mathbb{F}_\ell$, $\epsilon \in \mathcal{O}$ then $\ell\mathcal{O}\epsilon \subseteq \ell\mathcal{O}$, and $I_a\epsilon$ is left-$\mathcal{O}$ ideal, $\ell\mathcal{O} \subseteq I_a\epsilon$ (likely $\ell\mathcal{O} \subseteq I_a\bar{\epsilon}$). Then

$$\begin{aligned} I_a\epsilon &= \ell\mathcal{O}\epsilon + I(-1+(a+1)\epsilon) = \ell\mathcal{O} + \ell\mathcal{O}\epsilon + I(-1+(a+1)\epsilon) \\ &= \ell\mathcal{O} + I(-1+(a+1)\epsilon) = \ell\mathcal{O} + I(-(a+1)^{-1}+\epsilon) \\ &= I_{-(a+1)^{-1}}, \\ I_a\bar{\epsilon} &= \ell\mathcal{O}\bar{\epsilon} + I((a+1)-a\epsilon) = \ell\mathcal{O} + \ell\mathcal{O}\bar{\epsilon} + I((a+1)-a\epsilon) \\ &= \ell\mathcal{O} + I((a+1)-a\epsilon) = \ell\mathcal{O} + I(-(a+1)a^{-1}+\epsilon) \\ &= I_{-a^{-1}(a+1)}, \end{aligned}$$

where the second identity is by Lemma 7.

To summarize, we divide X_ℓ into $[\frac{\ell+2}{3}]$ subsets, each consisting of 2 or 3 elements in the same ideal class: $\{I, I_0, I_{-1}\}$, $\{I_a, I_{-(a+1)^{-1}}, I_{-a^{-1}(a+1)}\}$ $(a^2+a+1 \neq 0,1)$ and $\{I_b, I_{b^2}\}$ for $b^2+b+1=0$. We show that any two left ideals in different subsets are not in the same ideal class by contradiction.

Suppose I and J are from different subsets of X_ℓ and $I = J\mu$ for some $\mu \in B_{p,\infty}$, then $\mu \notin \{\pm 1, \pm\epsilon, \pm\bar{\epsilon}\}$ and $\mathrm{Nrd}(\mu) = 1$. Since $\ell \in J$, $\ell\mu \in I \subseteq \mathcal{O}$, and $\mu \in \ell^{-1}\mathcal{O}$. By Lemma 11(1), we have $\ell \equiv 1 \bmod 3$, $\mu = \frac{A+B\epsilon}{\ell}$, $A^2+AB+B^2 = \ell^2$ and $\ell \nmid A$. This means that $A + B\epsilon = u(m + n\frac{1\pm i}{2})^2$ for $u \in \{\pm 1, \pm\epsilon, \pm\bar{\epsilon}\}$, and thus $\gcd(A + B\epsilon, \ell)$ in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is $u(m + n\frac{1\pm i}{2})$. In particular $I_b = \mathcal{O}(m + n\epsilon) \subseteq I$ or $I_{b^2} = \mathcal{O}(m + n\bar{\epsilon}) \subseteq I$ and hence $I_b = I$ or $I_{b^2} = I$ as both are of the same reduced norm. Switch the role of I and J, we get $J = I_b$ or $J = I_{b^2}$. Hence both I and J are in the same subset $\{I_b, I_{b^2}\}$, impossible. By Deuring's Theorem (Theorem 6), and from Theorem 1, when $\ell \equiv 2 \bmod 3$, none of the subsets consist of ideals corresponding to endomorphisms. This completes the proof of the first part of Theorem 2(2).

For the second part, let E be a supersingular elliptic curve defined over $\mathbb{F}_p$ such that E_0 connects to E via a left $\mathcal{O}$-ideal of reduced norm ℓ. By [7, Proposition 2.4], a supersingular elliptic curve is defined over $\mathbb{F}_p$ if and only if $\mathbb{Z}[\sqrt{-p}]$ is contained in its endomorphism ring. Then $\mathrm{End}(E) = \mathcal{O}_R(I) \subseteq \ell^{-1}\mathcal{O}$ has an element s such that $s^2 = -p$. By Lemma 11(2), we know either $s \in \{\pm j, \pm\epsilon j, \pm\bar{\epsilon} j\}$ or in the case $\ell \equiv 1 \bmod 3$, $\ell s = xj + y\epsilon j$, $(x, y) \in \mathbb{Z}^2$ such that $\ell \nmid x$ and $x^2 + +xy + y^2 = \ell^2$.

Let $\hat{\mathcal{O}} = \mathcal{O}/\ell\mathcal{O}$. Then $\hat{\mathcal{O}}$ is a quaternion algebra over $\mathbb{F}_\ell$. We can identify $\hat{\mathcal{O}}$ with $M_2(\mathbb{F}_\ell)$ via the isomorphism θ in Theorem 5 with $q = 3$. Moreover, the set

$$\overline{X_\ell} = \{\hat{I}_\infty = M_2(\mathbb{F}_\ell)\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},\ \hat{I}_a := M_2(\mathbb{F}_\ell)\begin{pmatrix} 1 & 2a+1 \\ 0 & 0 \end{pmatrix}\ (a \in \mathbb{F}_\ell)\}$$

corresponds to X_ℓ bijectively. For our convenience, the form of the set $\overline{X_\ell}$ here is different from that in the proof of Theorem 5. Let I_a be the left $\mathcal{O}$-ideal of reduced norm ℓ corresponding to $\hat{I}_a$. For $s \in \mathcal{O}$, let $\hat{s}$ be the image of s in $M_2(\mathbb{F}_\ell)$. By abuse of notation, write i, j, k for $\hat{i}$, $\hat{j}$ and $\hat{k}$.

If $(\frac{-p}{\ell}) = 1$, let $t \in \mathbb{F}_\ell$ such that $t^2 = -p$ and let $(u, v) = (t, 0)$. In this case, $I_\infty = \mathcal{O}\ell + \mathcal{O}(-t + j)$, $I_a = \mathcal{O}\ell + \mathcal{O}(-t + j)(a + \epsilon)$. Then one can easily check that $\hat{I}_\infty j \subset \hat{I}_\infty$, $\hat{I}_{-2^{-1}} j \subset \hat{I}_{-2^{-1}}$ and $\hat{I}_a j \nsubseteq \hat{I}_a$ for all other a, this means $j \in \mathcal{O}_R(I_\infty)$, $j \in \mathcal{O}_R(I_{-2^{-1}})$ but

Table 1
The values of $P_1(\ell)$ and $P_2(\ell)$ for $5 \le \ell \le 200$.

ℓ	5	7	11	13	17	19	23	29	31	37	41
$P_1(\ell)$	83	191	479	659	1151	1439	2111	3359	3803	5471	6719
$P_2(\ell)$	47	71	311	479	839	1031	1559	2447	2711	4079	4967
Bound	I	I	I	×	I	I	I	I	×	I	I
ℓ	43	47	53	59	61	67	71	73	79	83	89
$P_1(\ell)$	7351	8831	11171	13907	14879	17939	20147	21227	24923	27551	31667
$P_2(\ell)$	5519	6599	8231	10391	11087	13259	14951	15959	18671	20639	23687
Bound	I	I, II	I	I	I	I	I	×	×	I	I
ℓ	97	101	103	107	109	113	127	131	137	139	149
$P_1(\ell)$	37619	40787	42407	45779	47507	51071	64499	68639	75011	77279	88799
$P_2(\ell)$	28151	30491	31799	34319	35591	38231	48311	51431	56099	57839	66491
Bound	I	I	I	I	I	I	I	I	I	I	I
ℓ	151	157	163	167	173	179	181	191	193	197	199
$P_1(\ell)$	91199	98543	106187	111539	119699	128159	130927	145879	148991	155231	158363
$P_2(\ell)$	68351	73823	79631	83639	89759	95819	98207	109391	111623	116351	118751
Bound	I	×	×	I	I	I	×	×	I	I	I

$j \notin \mathcal{O}_R(I_a)$ for other a. Similarly $\epsilon j \in \mathcal{O}_R(I_0), \mathcal{O}_R(I_{-2})$ and $\epsilon j \notin \mathcal{O}_R(I_a)$ for other a. Also, $\bar{\epsilon} j \in \mathcal{O}_R(I_{-1}), \mathcal{O}_R(I_1)$ and $\bar{\epsilon} j \notin \mathcal{O}_R(I_a)$ for other a. Now if $\ell \equiv 1 \bmod 3$ and (x, y) any solution that $x^2 + xy + y^2 = \ell^2$ and $\ell \nmid x$, then one can check $\hat{I}_a(\hat{x}j + \hat{y}\epsilon j) \neq 0$ if $a^2 + a + 1 \neq 0$, hence $\mathcal{O}(xj + y\epsilon j) \nsubseteq \ell\mathcal{O}$ and $\ell^{-1}(xj + y\epsilon j) \notin O_R(I_a)$ if $a^2 + a + 1 \neq 0$. If $a^2 + a + 1 = 0$, then $I_a = \mathcal{O}(m + n\epsilon)$ or $I_a = (m + n\bar{\epsilon})$ for $m^2 + mn + n^2 = \ell$, corresponding to the loops. In conclusion, there are two vertices defined over $\mathbb{F}_p$ adjacent to $[E_0]$, one corresponding to the ideal class $[I_\infty] = [I_0] = [I_{-1}]$ and the other corresponding to the ideal class $[I_1] = [I_{-2^{-1}}] = [I_{-2}]$.

If $(\frac{-p}{\ell}) = -1$, then $uv \neq 0$ for any solution (u, v) of $X^2 + 3Y^2 = -p$. It is easy to check $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) j \notin \hat{I}_\infty$. For $a \in \mathbb{F}_\ell$, $\left(\begin{smallmatrix} 1 & a \\ 0 & 0 \end{smallmatrix}\right) j \in \hat{I}_a$ implies that $2(2a + 1)u = (3 - (2a + 1)^2)v$. From $v \neq 0$, then $2a + 1 \neq 0$ and $u = \frac{3-(2a+1)^2}{2(2a+1)} v$. Hence $-p = \frac{(3+(2a+1)^2)^2}{(2(2a+1))^2} v^2$, impossible. This means $j \notin I_a$ for all $a \in \mathbb{F}_\ell \cup \{\infty\}$. Similarly $\epsilon j, \bar{\epsilon} j \notin I_a$ for all $a \in \mathbb{F}_\ell \cup \{\infty\}$. Also, if $x, y \neq 0$ such that $\begin{pmatrix} 1 & 2a+1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 2x + y & -3y \\ y & 2x + y \end{pmatrix} \begin{pmatrix} u & 3v \\ v & -u \end{pmatrix} = 0$, by computation, $a^2 + a + 1 = 0$, which corresponds to the loops. In conclusion, there is no vertex defined over $\mathbb{F}_p$ other than $[E_0]$. □

4. Numerical evidence

For a fixed prime $\ell > 3$, let $P_1(\ell)$ (resp. $P_2(\ell)$) be the largest prime p such that the number of vertices adjacent to $[E_{1728}]$ (resp. $[E_0]$) in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ is smaller than $\frac{1}{2}\left(\ell - (-1)^{\frac{\ell-1}{2}}\right)$ (resp. $\frac{1}{3}(\ell - (\frac{\ell}{3}))$), i.e., our main theorem fails for such a p. Let $P_1'(\ell)$ (resp. $P_2'(\ell)$) be the largest prime p such that $p \equiv 3 \bmod 4$ and $p < 4\ell^2$ (resp. $p \equiv 2 \bmod 3$ and $p < 3\ell^2$). By Theorem 2, $P_i(\ell) \le P_i'(\ell)$. The equality $P_1(\ell) = P_1'(\ell)$ (resp. $P_2(\ell) = P_2'(\ell)$) holds only when our bound $4\ell^2$ (resp. $3\ell^2$) is sharp, in this case we say Bound I (resp. Bound II) is satisfied for ℓ.

We compute the values of $P_1(\ell)$ and $P_2(\ell)$ for $5 \le \ell \le 200$ and list them in Table 1.

As can be seen from Table 1, of the 44 primes between 5 and 200, Bound I is satisfied for 36 primes. The prime 47 is the only $\ell < 200$ satisfying Bound II (and also Bound I), but the difference $P_2'(\ell) - P_2(\ell)$ for each ℓ is not big. In this sense our bounds are sharp.

5. The cases when $\ell = 2$ and 3

For completeness, we list results here for the cases $\ell = 2$ or 3.

(1) For the curve E_{1728} (hence $p \equiv 3 \bmod 4$),

$\ell = 2$ If $p > 4\ell = 8$, then $[E_{1728}]$ has 1 loop by [1, Theorem 10], and if I is non-principal of reduced norm ℓ, then $[I] = [I_0]$, $[E_{1728}]$ connects to another vertex by 2 edges; if $p = 7$, then $\Phi_2(X, 1728) \equiv (X - 1728)^3 \bmod 7$, $[E_{1728}]$ has 3 loops.

$\ell = 3$ If $p > 4\ell = 12$, then E_{1728} has no loop, and the 4 edges correspond to 2 ideal classes, $[E_{1728}]$ connects to 2 other vertices by 2 edges each; if $p = 7$, then $\Phi_3(X, 1728) \equiv (X + 1)^4 \bmod 7$, E_{1728} connects to another vertex by 4 edges; if $p = 11$, then $\Phi_3(X, 1728) \equiv (X^2 + X + 10)^2 \bmod 11$, which means E_{1728} connects to 2 vertices by 2 edges each.

(2) For the curve E_0 (hence $p \equiv 2 \bmod 3$),

$\ell = 2$ If $p > 3\ell = 6$, then E_0 has no loop by [12] and I, I_0, I_{-1} are in the same ideal class, which means $[E_0]$ connects to another vertex by 3 edges; if $p = 5$, then $\Phi_2(X, 0) \equiv X^3 \bmod 5$, which means $[E_0]$ has 3 loops.

$\ell = 3$ If $p > 3\ell = 9$, then $[E_0]$ has 1 loop by [12] and I, I_0, I_{-1} are in the same ideal class, which means $[E_0]$ connects to another vertex by 3 edges; if $p = 5$, then $\Phi_3(X, 0) \equiv X^4 \bmod 5$, which means $[E_0]$ has 4 loops.

Acknowledgment

Research is partially supported by Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200) and NSFC (Grant No. 11571328).

References

[1] G. Adj, O. Ahmadi, A. Menezes, On isogeny graphs of supersingular elliptic curves over finite fields, Finite Fields Appl. 55 (2019) 268–283.
[2] J.L. Alperin, R.B. Bell, Groups and Representations, GTM, vol. 162, Springer-Verlag, 1995.
[3] J. Biasse, D. Jao, A. Sankar, A quantum algorithm for computing isogenies between supersingular elliptic curves, in: W. Meier, D. Mukhopadhyay (Eds.), INDOCRYPT 2014, in: LNCS, vol. 8885, Springer, Berlin, 2014, pp. 428–442.
[4] A. Costache, B. Feigon, K. Lauter, M. Massierer, A. Puskas, Ramanujan Graphs in Cryptography, Cryptology ePrint Archive, Report 2018/593, 2018.
[5] A.M. Childs, D. Jao, V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, J. Math. Cryptol. 8 (2014) 1–29.
[6] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Semin. Univ. Hamb. 14 (1941) 197–272.

[7] C. Delfs, S. Galbraith, Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$, Des. Codes Cryptogr. 78 (2016) 425–440.
[8] J.M. Grau, C. Miguel, A.M. Oller-Marcen, On the structure of quaternion rings over $\mathbb{Z}/n\mathbb{Z}$, Adv. Appl. Clifford Algebras 25 (2015) 875–887.
[9] D. Jao, De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, in: B.-Y. Yang (Ed.), PQCrypto 2011, in: LNCS, vol. 7071, Springer, 2011, pp. 19–34.
[10] D. Kohel, K. Laute, C. Petit, J.P. Tignol, On the quaternion ℓ-isogeny path problem, LMS J. Comput. Math. 17A (2014) 418–432.
[11] K. McMurdy, Explicit representation of the endomorphism rings of supersingular elliptic curves, https://phobos.ramapo.edu/~kmcmurdy/research/McMurdy-ssEndoRings.pdf, 2014.
[12] Y. Ouyang, Z. Xu, Loops of isogeny graphs of supersingular elliptic curves at $j = 0$, Finite Fields Appl. 58 (2019) 174–176.
[13] J. Silverman, The Arithmetic of Elliptic Curves, second ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009.
[14] A. Stolbunov, Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, Adv. Math. Commun. 4 (2) (2010) 215–235.
[15] J. Voight, Quaternion algebras, v.0.9.15, May 26, 2019, available at https://www.math.dartmouth.edu/~jvoight/quat.html.