Finite Fields and Their Applications 62 (2020) 101619

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$

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

A R T I C L E   I N F O

Article history:
Received 30 July 2019
Received in revised form 1 November 2019
Accepted 7 November 2019
Available online xxxx
Communicated by Neal Koblitz

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

Keywords:
Supersingular elliptic curves over finite fields
Endomorphism ring
Isogeny graph

A B S T R A C T

Let $p > 3$ be a fixed prime. For a supersingular elliptic curve E over $\mathbb{F}_p$, a result of Ibukiyama tells us that $\mathrm{End}(E)$ is a maximal order $\mathcal{O}(q)$ (resp. $\mathcal{O}'(q)$) in $\mathrm{End}(E) \otimes \mathbb{Q}$ indexed by a (non-unique) prime q satisfying $q \equiv 3 \bmod 8$ and the quadratic residue $\left(\frac{p}{q}\right) = -1$ if $\frac{1+\pi}{2} \notin \mathrm{End}(E)$ (resp. $\frac{1+\pi}{2} \in \mathrm{End}(E)$), where $\pi = ((x, y) \mapsto (x^p, y^p)$ is the absolute Frobenius. Let q_j denote the minimal q for E whose j-invariant $j(E) = j$ and $M(p)$ denote the maximum of q_j for all supersingular $j \in \mathbb{F}_p$. Firstly, we determine the neighborhood of the vertex $[E]$ with $j \notin \{0, 1728\}$ in the supersingular ℓ-isogeny graph if $\frac{1+\pi}{2} \notin \mathrm{End}(E)$ and $p > q_j\ell^2$ or $\frac{1+\pi}{2} \in \mathrm{End}(E)$ and $p > 4q_j\ell^2$: there are either $\ell - 1$ or $\ell + 1$ neighbors of $[E]$, each of which connects to $[E]$ by one edge and at most two of which are defined over $\mathbb{F}_p$. We also give examples to illustrate that our bounds are tight. Next, under GRH, we obtain explicit upper and lower bounds for $M(p)$, which were not studied in the literature as far as we know. To make the bounds useful, we estimate the number of supersingular elliptic curves with $q_j < c\sqrt{p}$ for $c = 4$ or $\frac{1}{2}$. In the appendix, we compute $M(p)$ for all $p < 2000$ numerically.

* 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.2019.101619

Our data show that $M(p) > \sqrt{p}$ except $p = 11$ or 23 and $M(p) < p\log^2 p$ for all p.

1. Introduction

We fix a prime $p > 3$. Let $\ell \neq p$ be another fixed prime. The supersingular ℓ-isogeny graph $\mathscr{G}_\ell(\overline{\mathbb{F}}_p)$ is a directed graph, whose set of vertices $V_\ell(\overline{\mathbb{F}}_p)$ are $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curve $[E]$ defined over $\overline{\mathbb{F}}_p$ and whose edges are equivalent classes of ℓ-isogenies defined over $\overline{\mathbb{F}}_p$ between two elliptic curves in the isomorphism classes. As usual the vertices are represented by j-invariants. As seen in [17], $\mathscr{G}_\ell(\overline{\mathbb{F}}_p)$ is an expander graph, thus has good mixing propperties. Actually, finding paths between two vertices in $\mathscr{G}_\ell(\overline{\mathbb{F}}_p)$ is at least as hard as computing isogenies between supersingular elliptic curves, which is believed to be a hard problem. There are numerous works in cryptography based on this problem. Charles-Lauter-Goren [3] constructed hash functions from the supersingular isogeny graphs. Couveignes [2] first proposed isogeny crptosystems, Rostovtsev-Stolbunov [18] designed a public-key cryptosystem based on isogeny, Jao-De Feo [10] designed a Diffie-Hellman key exchange protocol as a candidate for a post-quantum key exchange, Galbraith-Petit-Silva [12] proposed an identification scheme and a signature scheme, Castryck-Lange-Martindale [4] proposed a non-interactive key exchange in a post-quantum setting.

In 2016, Delfs-Galbraith [9] studied the supersingular ℓ-isogeny graph where the isomorphism classes and isogenies are all defined over $\mathbb{F}_p$. In 2019, Adj [1] computed the subgraphs $\mathscr{G}_\ell(\mathbb{F}_{p^2}, t)$ with vertices representing elliptic curves of trace $t \in \{0, \pm p\}$ and edges are defined over $\mathbb{F}_{p^2}$. They also obtained information for the loops of $j = 0$ and $j = 1728$ when $p > 4\ell$. This bound was improved to $p > 3\ell$ when $j = 0$ by two of us in [16]. In a subsequent work [14], we determined the neighborhood of $[E_{1728}]$ if $p > 4\ell^2$ and $[E_0]$ if $p > 3\ell^2$ in $\mathscr{G}_\ell(\overline{\mathbb{F}}_p)$. In this note, we shall work on the supersingular elliptic curves with j-invariants in $\mathbb{F}_p \backslash \{0, 1728\}$. From now on, if $j \in \mathbb{F}_p$ is a supersingular j-invariant, we pick one supersingular elliptic curve E_j over $\mathbb{F}_p$ with $j(E_j) = j$. For any elliptic curve E, the kernel of an ℓ-isogeny starting from E is a subgroup of $E[\ell]$ of cardinality ℓ, and there are $\ell + 1$ distinct subgroups of cardinality ℓ in $E[\ell]$. Thus there are $\ell + 1$ edges connecting $[E_j]$ in $\mathscr{G}_\ell(\overline{\mathbb{F}}_p)$. In Theorem 1.1 we shall determine the neighborhood of $[E_j]$ for $j \in \mathbb{F}_p \backslash \{0, 1728\}$ in $\mathscr{G}_\ell(\overline{\mathbb{F}}_p)$ when certain bounds are satisfied for the prime p, and in particular we shall determine the $\mathbb{F}_p$-neighbors of $[E_j]$. Moreover, we show that the bounds in Theorem 1.1 are tight. To state our main results, we need to make some preparation in the following.

It is well-known (see [19]) that every supersingular elliptic curve over $\overline{\mathbb{F}}_p$ has j-invariant in $\mathbb{F}_{p^2}$, thus $V_\ell(\overline{\mathbb{F}}_p) = V_\ell(\mathbb{F}_{p^2})$ and further investigation tells us that its cardinality is $\lfloor \frac{p}{12} \rfloor + \varepsilon$ where $\varepsilon = 0$, 1 or 2 depending on the class of $p \mod 12$. For supersingular elliptic curves over $\mathbb{F}_p$, one has (see [9] or [7, Theorem 14.18])

$$\#\{\jmath \in \mathbb{F}_p \mid \jmath \text{ is a supersingular invariant}\} = \begin{cases} \frac{1}{2}h(-p), & \text{if } p \equiv 1 \bmod 4, \\ h(-p), & \text{if } p \equiv 7 \bmod 8, \\ 2h(-p), & \text{if } p \equiv 3 \bmod 8, \end{cases}$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$. Moreover, when $p \to \infty$, by the Brauer-Siegel Theorem ([6, Theorem 4.9.15]), $h(-p)$ is approximately $\sqrt{p}$ or $2\sqrt{p}$ if $p \equiv 3$ or $1 \bmod 4$.

For a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, its endomorphism ring $\mathrm{End}(E)$ is a maximal order in the unique definite quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified only at p and ∞ (see [21]). Furthermore $\jmath(E) \in \mathbb{F}_p$ if and only if $\mathrm{End}(E)$ contains a root of $x^2+p=0$. If $\jmath \in \mathbb{F}_p \backslash \{0, 1728\}$ is a supersingular $\jmath$-invariant, let $\pi = ((x,y) \mapsto (x^p, y^p))$ be the absolute Frobenius in $\mathrm{End}(E_\jmath)$, it can be shown that $\pm\pi$ are the only roots of x^2+p in $\mathrm{End}(E_\jmath)$.

For q a prime satisfying $q \equiv 3 \bmod 8$ and the quadratic residue $\left(\frac{p}{q}\right) = -1$, let $H(-q,-p) = \mathbb{Q}\langle 1, i, j, k\rangle$ be the quaternion algebra over $\mathbb{Q}$ defined by $i^2 = -q$, $j^2 = -p$ and $ij = -ji = k$. By computing the discriminant of $H(-q,-p)$ one sees that $B_{p,\infty} \cong H(-q,-p)$. We identify these two quaternion algebras by the isomorphism. Let

$$\mathcal{O}(q) := \mathbb{Z}\langle 1, \frac{1+i}{2}, \frac{j+k}{2}, \frac{ri-k}{q}\rangle \text{ where } r^2+p \equiv 0 \bmod q,$$

and allowing also $q = 1$,

$$\mathcal{O}'(q) := \mathbb{Z}\langle 1, \frac{1+j}{2}, i, \frac{r'i-k}{2q}\rangle \text{ where } p \equiv 3 \bmod 4,\ r'^2+p \equiv 0 \bmod 4q.$$

Then $\mathcal{O}(q)$ and $\mathcal{O}'(q)$ are maximal orders in $B_{p,\infty}$. Note that the choices of r and r' in $\mathbb{Z}$ are not essential, up to isomorphism the orders $\mathcal{O}(q)$ and $\mathcal{O}'(q)$ depend only on q (and of course p). Then for $\jmath \in \mathbb{F}_p$ a supersingular $\jmath$-invariant, Ibukiyama [13] showed that $\mathrm{End}(E_\jmath)$ is isomorphic to $\mathcal{O}(q)$ if $\frac{1+\pi}{2} \notin \mathrm{End}(E_\jmath)$ (equivalently, $\mathrm{End}(E_\jmath) \cap \mathbb{Q}(\pi) = \mathbb{Z}[\pi]$) or $\mathcal{O}'(q)$ if $\frac{1+\pi}{2} \in \mathrm{End}(E_\jmath)$ (equivalently, $\mathrm{End}(E_\jmath) \cap \mathbb{Q}(\pi) = \mathbb{Z}[\frac{1+\pi}{2}]$) for some q. In particular, $\mathrm{End}(E_0) \cong \mathcal{O}(3)$ and $\mathrm{End}(E_{1728}) \cong \mathcal{O}'(1)$.

However, q is not unique. Let $q_\jmath$ be minimal such that $\mathrm{End}(E_\jmath) \cong \mathcal{O}(q_\jmath)$ or $\mathcal{O}'(q_\jmath)$. Certainly $q_0 = 3$ and $q_{1728} = 1$. When $q_\jmath$ is small compared to p, we can apply the techniques in our previous work [14] to determine the neighborhood of $[E_\jmath]$ in the supersingular isogeny graph. Let $H_D(x) \in \mathbb{Z}[x]$ be the Hilbert class polynomial of an imaginary quadratic order with discriminant D. Define

$$\delta_D = \begin{cases} 1, & \text{if } \left(\frac{D}{\ell}\right) = 1 \text{ and } H_D(x) \text{ splits into linear factors in } \mathbb{F}_\ell[x]; \\ -1, & \text{otherwise.} \end{cases}$$

We have

Theorem 1.1. *Let* $j \in \mathbb{F}_p \backslash \{0, 1728\}$ *be a supersingular* j*-invariant and* π *be the Frobenius map of* E_j*. Suppose* $\ell \nmid 2pq_j$*.*

(i) *In the case* $\frac{1+\pi}{2} \notin \mathrm{End}(E_j)$*, i.e.* $\mathrm{End}(E_j) = \mathcal{O}(q_j)$*, if* $p > q_j \ell^2$*, there are* $1 + \delta_{-q_j}$ *loops of* $[E_j]$ *and* $\ell - \delta_{-q_j}$ *vertices adjacent to* $[E_j]$ *in* $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ *and hence each connecting to* $[E_j]$ *by one edge.*

(ii) *In the case* $\frac{1+\pi}{2} \in \mathrm{End}(E_j)$*, i.e.* $\mathrm{End}(E_j) = \mathcal{O}'(q_j)$*, if* $p > 4q_j \ell^2$*, there are* $1 + \delta_{-4q_j}$ *loops of* $[E_j]$ *and* $\ell - \delta_{-4q_j}$ *vertices adjacent to* $[E_j]$ *in* $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ *and hence each connecting to* $[E_j]$ *by one edge.*

In both cases, there are $1 + \left(\frac{-p}{\ell}\right)$ *vertices defined over* $\mathbb{F}_p$ *adjacent to* $[E]$ *with one* $\mathbb{F}_p$*-edge.*

Remark 1.2. Fix ℓ and q, the lower bound $q\ell^2$ or $4q\ell^2$ for p is sharp, just like the cases considered in [14]. We have two examples. In both cases, the result in Theorem 1.1 does not hold when the bound is not satisfied.

(1) Let $q = 11$, $\ell = 13$. Then $p = 1847$ is the largest prime such that $\left(\frac{-p}{q}\right) = 1$ and $p < q\ell^2$. Let $E : y^2 = x^3 + 1594x + 447$, then E is a supersingular elliptic curve defined over $\mathbb{F}_{1847}$ with $\mathrm{End}(E) \cong \mathcal{O}(11)$. By computation, $[E]$ has three neighbors $j_1 = 1336$, $j_2 = 319$ and $j_3 = 437$ defined over $\mathbb{F}_{1847}$ in $\mathcal{G}_{13}(\overline{\mathbb{F}}_{1847})$, which is larger than $1 + \left(\frac{-p}{\ell}\right) = 2$. Moreover, the multiplicity of edge between E and E_{437} is 2, and there are 13 vertices adjacent to $[E]$.

(2) Let $q = 3$, $\ell = 5$. Then $p = 293$ is the largest prime such that $\left(\frac{-p}{q}\right) = 1$ and $p < 4q\ell^2$. Let $E : y^2 = x^3 + 256x + 73$, then E is supersingular over $\mathbb{F}_{293}$ with $\mathrm{End}(E) \cong \mathcal{O}'(3)$. $[E]$ has no loops but one neighbor $j_1 = 212$ defined over $\mathbb{F}_{293}$ in $\mathcal{G}_5(\overline{\mathbb{F}_{293}})$ which is larger than $1 + \left(\frac{-p}{\ell}\right) = 0$. Moreover, the multiplicity of edge between E and E_{212} is 2, and there are 5 vertices adjacent to $[E]$.

Unfortunately, numerical evidence tells us that q_j might be larger than p. Let $M(p) = \max\{q_j \mid j \text{ is a supersingular invariant over } \mathbb{F}_p\}$. In the appendix we collect data of $M(p)$ for $p < 2000$, which reveal that $M(p) > \sqrt{p}$ except $p = 11$ or 23 and $M(p) < p \log^2 p$ for all p. Under Generalized Riemann Hypothesis (GRH), we obtain the following result.

Theorem 1.3. *Let* $p > 3$ *be a prime. Assume GRH (Generalized Riemann Hypothesis) holds.*

(1) *For any constant* $C > 0$*, if* p *is sufficiently large, there exists a supersingular invariant* j *such that* $q_j > C\sqrt{p}$*.*

(2) *For a generic supersingular* j*-invariant* $j \in \mathbb{F}_p \backslash \{0, 1728\}$*,* $q_j < 10000p \log^4 p$*.*

(3) *For any supersingular* j*-invariant* $j \in \mathbb{F}_p \backslash \{0, 1728\}$*,* $q_j < 10000p \log^6 p$*.*

(4) *Let* $N(x) = \#\{q_j \leq x \mid j \text{ is a supersingular } j\text{-invariant in } \mathbb{F}_p\}$*. Then*

(i) *If* $p \equiv 1 \bmod 4$, *then* $N(4\sqrt{p}) \sim \frac{\sqrt{p}}{\log p}$ *as* $p \to \infty$.
(ii) *If* $p \equiv 3 \bmod 4$, *then* $N(\frac{\sqrt{p}}{2}) \sim \frac{\sqrt{p}}{4\log p}$ *as* $p \to \infty$ *and* $\liminf N(4\sqrt{p})\frac{\log p}{\sqrt{p}} \geq \frac{9}{8}$.

Acknowledgments

Research is partially supported by Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200) and NSFC (Grant No. 11571328). Y.O. would like to thank the Morningside Center of Mathematics for hospitality where part of this paper was written. The authors also would like to thank the reviewers heartfully for valuable comments and suggestions.

2. Preliminaries

2.1. Elliptic curves over finite fields

In this subsection, we introduce some basic knowledge about elliptic curves over finite fields, one can refer to [19] for details. Let $\mathbb{F}$ be a finite field of characteristic $p > 3$, let $\bar{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$. An elliptic curve E defined over $\mathbb{F}$ is a projective curve with affine model $E : y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{F}$ and $4A^3 + 27B^2 \neq 0$. The j-invariant of E is $j(E) = 1728\frac{4A^3}{4A^3+27B^2}$. The set of $\mathbb{F}$-rational points on E is $E(\mathbb{F}) = \{(x, y) \in \mathbb{F}^2 : y^2 = x^3 + Ax + B\} \cup \{\infty\}$, where ∞ is the point at infinity. Then $E(\mathbb{F})$ is a finite abelian group.

Let E and E' be two elliptic curves defined over $\mathbb{F}$. An isogeny $\phi : E \to E'$ is a morphism satisfying $\phi(\infty) = \infty$. If $\phi(E) = \{\infty\}$, we say $\phi = 0$. If $\phi \neq 0$, then ϕ is a surjective group homomorphism with finite kernel, and we call E and E' isogenous. The isogeny ϕ is called an L-isogeny if it is defined over L (i.e. written as rational maps over L), ϕ is called separable (resp. inseparable) if the corresponding field extension $\overline{\mathbb{F}}(E)/\phi^*\overline{\mathbb{F}}(E')$ is separable (resp. inseparable). The degree of ϕ is the degree of the field extension $\overline{\mathbb{F}}(E)/\phi^*\overline{\mathbb{F}}(E')$. If ϕ is separable, in particular if $p \nmid \deg\phi$, then $\deg(\phi) = \#\ker(\phi)$. If $\deg(\phi) = 1$, E and E' are isomorphic. Particularly, if $j(E) = j(E')$, then E and E' are isomorphic over $\overline{\mathbb{F}}$.

An endomorphism of E is an isogeny from E to itself. The set $\mathrm{End}(E)$ of all endomorphisms of E form a ring under the usual addition and composition as multiplication. As in [19], $\mathrm{End}(E)$ is either an order in an imaginary quadratic extension of $\mathbb{Q}$ or a maximal order in a quaternion algebra over $\mathbb{Q}$. In the first case E is called ordinary, in the second case E is called supersingular. Moreover, every supersingular elliptic curve over $\overline{\mathbb{F}}_p$ is isomorphic to an elliptic curve defined over $\mathbb{F}_{p^2}$. Consequently, we may and will assume the supersingular elliptic curve E we study is defined over $\mathbb{F}_{p^2}$.

2.2. Number theoretic background

In this subsection, we introduce some basic knowledge in number theory needed later. Most of it can be found in [15,7,20]. We shall use big O to denote an order in a number field and calligraphic $\mathscr{O}$ to denote an order in a quaternion algebra over $\mathbb{Q}$ as in § 2.3.

For M a number field, let O_M, I_M, P_M and h_M be the ring of integers, the group of fractional ideals, the group of principal ideals and the class number of M.

Let M/N be an extension of number fields of degree $[M:N]=m$. Then O_M is a free O_N-module of rank m. Let $\{e_1,\cdots,e_m\}$ be a basis of O_M over O_N and $\{\sigma_1,\cdots,\sigma_m\}$ be the set of N-embeddings of M in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, then the discriminant $D_{M/N} := (\det(\sigma_i(e_j))_{i,j})^2 \in O_N$. Let O_M^* be the dual O_N-module of O_M under the trace map, then the different $\mathfrak{D}_{M/N}$ is the inverse of O_M^*, which is an ideal of O_M. We write $D_{M/\mathbb{Q}} = D_M$.

Proposition 2.1. *Suppose M/N is an extension of number fields. Then*

$$N_{M/N}(\mathfrak{D}_{M/N}) = D_{M/N},$$

where $N_{M/N}: M \to N$ is the norm map. Moreover,

(i) *If L is an intermediate field in M/N, then*

$$\mathfrak{D}_{M/N} = \mathfrak{D}_{M/L}\cdot\mathfrak{D}_{L/N}, \quad D_{M/N} = (D_{L/N})^{[M:L]}\cdot N_{L/N}(D_{M/L}).$$

(ii) *Let M_1 and M_2 be number fields, $N = M_1\cap M_2$ and $M = M_1M_2$. Suppose M_1 and M_1 are linearly disjoint over N, i.e. $[M:N] = [M_1:N]\cdot[M_2:N]$. Then*

$$\mathfrak{D}_{M/N} \mid \mathfrak{D}_{M_1/N}\mathfrak{D}_{M_2/N}, \quad D_{M/N} \;\Big|\; D_{M_1/N}^{[M:M_1]}\cdot D_{M_2/N}^{[M:M_2]}.$$

If $D_{M_1/N}$ and $D_{M_2/N}$ are moreover coprime, then

$$\mathfrak{D}_{M/N} = \mathfrak{D}_{M_1/N}\mathfrak{D}_{M_2/N}, \quad D_{M/N} = (D_{M_1/N})^{[M_2:N]}\cdot(D_{M_2/N})^{[M_1:N]}.$$

Proof. All are standard facts, except the first part of (ii), which we prove here for lack of reference. By (i), $\mathfrak{D}_{M/N} = \mathfrak{D}_{M/M_1}\mathfrak{D}_{M_1/N}$. By assumption, an N-embedding $\sigma: M_2 \hookrightarrow \overline{\mathbb{Q}}$ extends uniquely to an M_1-embedding $M \hookrightarrow \overline{\mathbb{Q}}$. If $\{e_1,\cdots,e_n\}$ is a basis of O_{M_2} over O_N, let R be the O_{M_1}-submodule of O_M generated by $\{e_1,\cdots,e_n\}$. By definition, under the trace map of M/M_1, R^* is $(\mathfrak{D}_{M_2/N}O_M)^{-1}$, O_M^* is $\mathfrak{D}_{M/M_1}^{-1}$, hence we have $\mathfrak{D}_{M/M_1} \mid \mathfrak{D}_{M_2/N}$. $\square$

For a Galois extension M/N of number fields, let $\mathfrak{p}$ be a prime ideal of O_N and $\mathfrak{P}$ a prime of O_M lying above $\mathfrak{p}$. Suppose $\mathfrak{P}/\mathfrak{p}$ is unramified. The Frobenius automorphism $\left[\frac{M/N}{\mathfrak{P}}\right]$ is the unique element $\sigma \in G = \mathrm{Gal}(M/N)$ such that

$$\sigma(\alpha) = \alpha^{N(\mathfrak{p})} \mod \mathfrak{P} \text{ for all } \alpha \in O_M$$

where $N(\mathfrak{p}) = \#(O_N/\mathfrak{p})$. All $[\frac{M/N}{\mathfrak{P}}]$, when $\mathfrak{P}$ varies over primes above $\mathfrak{p}$, form a conjugate class in $\mathrm{Gal}(M/N)$, which we denote by $[\frac{M/N}{\mathfrak{p}}]$. In the special case that M/N is an abelian extension, $[\frac{M/N}{\mathfrak{p}}] = [\frac{M/N}{\mathfrak{P}}]$ is a one-point-set.

For C a conjugacy class in G, define the function

$$\pi_C(x, M/N) := \#\{\mathfrak{p} \mid \mathfrak{p} \text{ is unramified in } M,\ [\frac{M/N}{\mathfrak{p}}] = C,\ N(\mathfrak{p}) \le x\}. \tag{2.2.1}$$

We have the following explicit Chebotarev density theorem:

Theorem 2.2. *For any conjugacy class C of $G = \mathrm{Gal}(M/N)$, the set of primes $\mathfrak{p}$ in N such that $[\frac{M/N}{\mathfrak{p}}] = C$ is of density $\frac{|C|}{|G|}$, i.e.,*

$$\pi_C(x, M/N) \sim \frac{|C|}{|G|}\frac{x}{\log(x)}.$$

More explicitly, let $n_M = [M : \mathbb{Q}]$ and $d_M = |D_M|$, then under GRH, one has

$$\Big|\frac{|G|}{|C|}\pi_C(x, M/N) - \int_2^x \frac{dt}{\log t}\Big| \le \sqrt{x}\left[\Big(\frac{1}{2\pi} + \frac{3}{\log x}\Big)\log d_M + \Big(\frac{\log x}{8\pi} + \frac{1}{4\pi} + \frac{6}{\log x}\Big)n_M\right]. \tag{2.2.2}$$

Proof. The first part can be found in any advanced number theory textbook. The explicit formula in the second part is a recent result in [11]. $\square$

Let K be an imaginary quadratic field. Let O be an order of K. The conductor of O is $f = [O_K : O]$, and the discriminant of O is $D(O) = f^2 D_K$. In general O may not be a Dedekind domain if $f > 1$, however for any O-ideal $\mathfrak{a}$ prime to f, $\mathfrak{a}$ has a unique decomposition as a product of prime O-ideals which are prime to f (see [7, Proposition 7.20]).

Let $I(O)$ be the group of proper fractional O-ideals prime to f and $P(O)$ be the group of principal fractional O-ideals prime to f, then the ideal class group of O is $\mathrm{cl}(O) = I(O)/P(O)$ and the ideal class number of O is $h(O) = \#\mathrm{cl}(O)$. Let $I_K(f)$ be the group of fractional O_K-ideals prime to f and $P_K(f)$ be the principal ideals in $I_K(f)$. Let $P_{K,\mathbb{Z}}(f)$ be the group of principal ideals in $P_K(f)$ generated by x with $x \equiv n \bmod fO_K$ for $n \in \mathbb{Z}$ (and relatively prime to f). The group $\mathrm{cl}(O)$ is canonically isomorphic to the ring class group $I_K(f)/P_{K,\mathbb{Z}}(f)$. The ring class field L of O is the (unique) abelian extension of K associated by the existence theorem of class field theory to the ring class group of O. The Artin map $\sigma : \mathrm{cl}(O) \cong \mathrm{Gal}(L/K)$ is the canonical isomorphism sending the class of $\mathfrak{p}$ to the Frobenius automorphism $[\frac{L/K}{\mathfrak{p}}]$. Moreover, the uniqueness implies that L is Galois over $\mathbb{Q}$.

For a lattice $\Lambda \subseteq \mathbb{C}$, let E_Λ be the elliptic curve over $\mathbb{C}$ such that $E_\Lambda(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Then $E_\Lambda \cong E_{\Lambda'}$ (i.e. $j(E_\Lambda) = j(E_{\Lambda'})$) if and only if $\Lambda = \lambda\Lambda$ for some $\lambda \in \mathbb{C}^\times$ (i.e. Λ and Λ' are homothetic). For O an order in an imaginary quadratic field K, let

$$\mathrm{Ell}_O(\mathbb{C}) := \{j(E) \mid \mathrm{End}(E) \cong O\} \quad (= \{E \mid \mathrm{End}(E) \cong O\}/\sim).$$

Then $\mathrm{Ell}_O(\mathbb{C}) = \{j(E_\mathfrak{b}) \mid [\mathfrak{b}] \in \mathrm{cl}(O)\}$ and $\mathrm{cl}(O)$ acts transitively on $\mathrm{Ell}_O(\mathbb{C})$ by $[\mathfrak{a}]j(E_\mathfrak{b}) = j(E_{\mathfrak{a}^{-1}\mathfrak{b}})$ (see [20, Chapter 18]). On the other hand the Galois group $\mathrm{Gal}(L/K)$ acts naturally on $\mathrm{Ell}_O(\mathbb{C})$. These two actions are compatible with the canonical isomorphism $\sigma : \mathrm{cl}(O) \cong \mathrm{Gal}(L/K)$ (see [20, Theorem 22.1]).

Now suppose O is of discriminant D. The Hilbert class polynomial $H_D(x)$ is defined as

$$H_D(x) := \prod_{j(E)\in \mathrm{Ell}_O(\mathbb{C})} (x - j(E)).$$

From [20, Theorem 21.12], $H_D(x) \in \mathbb{Z}[x]$. The splitting field of $H_D(x)$ over K is exactly the ring class field L of O. One has the following theorem ([20, Theorem 22.5]):

Theorem 2.3. *Let O be an imaginary quadratic order of discriminant D and L its ring class field. Let $\ell \nmid D$ be an odd prime which is unramified in L. Then the following are equivalent:*

(i) *ℓ is the norm of a principal O-ideal.*
(ii) *The Legendre symbol $\left(\frac{D}{\ell}\right) = 1$ and $H_D(x)$ splits into linear factors in $\mathbb{F}_\ell[x]$.*
(iii) *ℓ splits completely in L.*
(iv) *$4\ell = t^2 - v^2D$ for some integers t and v with $\ell \nmid t$.*

2.3. Quaternion algebras and maximal orders

Recall that a definite quaternion algebra over $\mathbb{Q}$ is of the form

$$H(-a,-b) = \mathbb{Q}\langle 1,i,j,k\rangle,\ i^2 = -a,\ j^2 = -b,\ k = ij = -ji$$

for some positive integers a and b. A lattice in $H(-a,-b)$ is a $\mathbb{Z}$-submodule of $H(-a,-b)$ of rank 4 containing a basis of $H(-a,-b)$. There is a canonical involution on $H(-a,-b)$ defined as

$$\alpha = x + yi + zj + wk \mapsto \bar{\alpha} = x - yi - zj - wk, \text{ for all } \alpha \in H(-a,-b).$$

The reduced trace of α is $\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2x$ and the reduced norm of α is $\mathrm{Nrd}(\alpha) = \alpha\bar{\alpha} = x^2 + ay^2 + bz^2 + abw^2$.

Let $B_{p,\infty} = H(-1,-p)$ be the unique quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞. However, one must keep in mind that there are many pairs of (a,b) such that $B_{p,\infty} = H(-a,-b)$, but the involution and hence the reduced trace and norm of $\alpha \in B_{p,\infty}$ are independent of the choice of (a,b).

An order $\mathcal{O}$ in $B_{p,\infty}$ is a lattice which is also a subring of $B_{p,\infty}$. The order $\mathcal{O}$ is called maximal if it is not properly contained in any other order. For two orders $\mathcal{O}$ and $\mathcal{O}'$ of $B_{p,\infty}$, we say that they are isomorphic if there exists $\mu \in B_{p,\infty}^{\times}$ such that $\mathcal{O}' = \mu\mathcal{O}\mu^{-1}$.

For a sublattice $I \subseteq B_{p,\infty}$, we define the left order of I by $\mathcal{O}_L(I) = \{x \in B_{p,\infty} \mid xI \subseteq I\}$ and the right order of I by $\mathcal{O}_R(I) = \{x \in B_{p,\infty} \mid Ix \subseteq I\}$. If $\mathcal{O}$ is a maximal order and I is a left ideal of $\mathcal{O}$, then $\mathcal{O}_L(I) = \mathcal{O}$ and $\mathcal{O}_R(I)$ is also a maximal order. For I a left ideal of $\mathcal{O}$, define the reduced norm of I by

$$\mathrm{Nrd}(I) = \gcd\{\mathrm{Nrd}(\alpha)|\ \alpha \in I\} = \sqrt{\mathcal{O}/I},$$

and define the conjugation ideal of I by $\bar{I} = \{\bar{\alpha} \mid \alpha \in I\}$. Then $\mathrm{Nrd}(\bar{I}) = \mathrm{Nrd}(I)$ and

$$I\bar{I} = \mathrm{Nrd}(I)\mathcal{O} = \mathrm{Nrd}(\bar{I})\mathcal{O}_R(\bar{I}).$$

2.4. Deuring's correspondence

Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. From [21], $\mathrm{End}(E) = \mathcal{O}$ is a maximal order in $B_{p,\infty} = \mathrm{End}(E) \otimes \mathbb{Q}$. For I a left ideal of $\mathcal{O}$, let $E[I] = \{P \in E(\overline{\mathbb{F}}_{\mathrm{p}}) \mid \alpha(P) = \infty$ for all $\alpha \in I\}$, then the quotient map

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

is an isogeny with $\deg(\phi_I) = \mathrm{Nrd}(I)$. On the other hand, if $\phi : E \to E'$ is an isogeny of degree N, then $\ker\phi$ is of order N and $I_\phi = \{\alpha \in \mathcal{O} \mid \alpha(P) = \infty \text{ for all } P \in \ker\varphi\}$ is a left $\mathcal{O}$-ideal of reduced norm N, and there exists an isomorphism $\psi : E_{I_\phi} \cong E'$ such that $\phi = \psi \circ \phi_I$. Then the following results of Deuring hold (see [21, Chapter 42], [8]).

Theorem 2.4. *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 (up to isomorphism) in $B_{p,\infty}$.*

(i) *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 $[\phi] \mapsto I_\phi$.*

(ii) *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.*

(iii) *Suppose $\phi_I : E \to E_I$ and $\phi_J : E \to E_J$ are isogenies corresponding to the left ideals I and J of $\mathcal{O}$ respectively. Then $E_I \cong E_J$ if and only if I and J are in the same left class of $\mathcal{O}$, i.e., $J = I\mu$ for some $\mu \in B_{p,\infty}^{\times}$.*

Conversely, from [21, Lemma 42.4.1], let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$, then $\mathcal{O} \cong \mathrm{End}(E)$ for some supersingular elliptic curve E over $\mathbb{F}_{p^2}$. More precisely, we have

Lemma 2.5. *Let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$. Then there exist one or two supersingular elliptic curves E up to isomorphism over $\overline{\mathbb{F}}_p$ such that $\mathrm{End}(E) \cong \mathcal{O}$. There exist two such elliptic curves if and only if $j(E) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$.*

Lemma 2.6. *Suppose E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Then E is defined over $\mathbb{F}_p$ if and only if that $\mathrm{End}(E)$ contains an element with minimal polynomial $x^2 + p$. Moreover, if $j(E) \neq 0, 1728$, then the absolute Frobenius $\pi = ((x, y) \mapsto (x^p, y^p)) \in \mathrm{End}(E)$ is the only isogeny up to a sign satisfying $x^2 + p = 0$.*

Proof. The equivalence follows from [9, Proposition 2.4].

Suppose that $\phi \in \mathrm{End}(E)$ satisfying $\phi^2 = [-p]$. Then $\hat{\phi} = -\phi$ and $\hat{\phi} \circ \phi = [p]$. Since E is supersingular, $E[p] = \{\infty\}$, thus $\ker \phi = \{\infty\}$ and ϕ is inseparable. From [19, Corollary 2.12], $\phi = \lambda \circ \pi$, where $\lambda \in \mathrm{End}(E)$. Then $\deg(\lambda) = 1$. From [19, Corollary 2.4.1], $\lambda \in \mathrm{Aut}(E) = \{\pm 1\}$ when $j(E) \neq 0$ or 1728. Thus $\phi = \pm\pi$. $\square$

Ibukiyama [13] has given an explicit description of all maximal orders $\mathcal{O}$ in $B_{p,\infty}$ containing a root ϵ of $x^2 + p = 0$. Regard $\mathcal{O}$ and $\mathbb{Q}(\epsilon)$ as subsets in $B_{p,\infty}$, then $\mathbb{Q}(\epsilon) \cap \mathcal{O}$ is either $\mathbb{Z}[\epsilon] \cong \mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}[\frac{1+\epsilon}{2}] \cong \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ where in the latter case $p \equiv 3 \bmod 4$. Let q be a prime such that

$$\left(\frac{p}{q}\right) = -1, \quad q \equiv 3 \mod 8. \tag{2.4.1}$$

Then the definite quaternion algebra $H(-q, -p) = \mathbb{Q}\langle 1, i, j, k\rangle$ with $i^2 = -q$, $j^2 = -p$ and $k = ij = -ji$ is also ramified only at p and ∞ and we can identify it with $B_{p,\infty}$. By (2.4.1), $\left(\frac{-p}{q}\right) = 1$. Let r be an integer such that $r^2 + p \equiv 0 \mod q$ and

$$\mathcal{O}(q) := \mathbb{Z}\langle 1, \frac{1+i}{2}, \frac{j-k}{2}, \frac{ri-k}{q}\rangle.$$

If $p \equiv 3 \mod 4$ and we allow $q = 1$, let r' be an integer such that $r'^2 + p \equiv 0 \mod 4q$ and

$$\mathcal{O}'(q) := \mathbb{Z}\langle 1, \frac{1+j}{2}, i, \frac{r'i-k}{2q}\rangle.$$

Then $\mathcal{O}(q)$ and $\mathcal{O}'(q)$ are maximal orders in $B_{p,\infty}$ which are independent of the choices of r and r' up to isomorphism. From [13], we have

Theorem 2.7. *Assume that $\mathcal{O}$ is a maximal order in $B_{p,\infty}$ containing an element ϵ with minimal polynomial $x^2 + p$. Then there exists a prime q satisfying condition (2.4.1) such* *that* $\mathcal{O} \cong \mathcal{O}(q)$ *if* $\mathcal{O} \cap \mathbb{Q}(\epsilon) = \mathbb{Z}[\epsilon]$ *and* $\mathcal{O} \cong \mathcal{O}'(q)$ *or* $\mathcal{O}'(1)$ *if* $\mathcal{O} \cap \mathbb{Q}(\epsilon) = \mathbb{Z}[\frac{1+\epsilon}{2}]$ *(hence* $p \equiv 3 \mod 4$*).*

Remark 2.8. Given a maximal order $\mathcal{O}$ in the form of $\mathcal{O}(q)$ or $\mathcal{O}'(q)$ in $B_{p,\infty}$, by Lemma 2.5, $\mathcal{O}$ corresponds to a supersingular elliptic curve E over $\mathbb{F}_p$ such that $\mathcal{O} \cong \mathrm{End}(E)$. Chevyrev and Galbraith [5] proposed an algorithm to compute this supersingular elliptic curve with running time $O(p^{1+\epsilon})$.

Let $\jmath \in \mathbb{F}_p$ be a supersingular $\jmath$-invariant and $E_\jmath$ be the corresponding supersingular elliptic curve defined over $\mathbb{F}_p$. Then $\mathrm{End}(E_0) \cong \mathcal{O}(3)$ and $\mathrm{End}(E_{1728}) \cong \mathcal{O}'(1)$. If $\jmath \neq 0, 1728$, then by Theorem 2.7 and Lemma 2.6, $\mathrm{End}(E_\jmath) \cong \mathcal{O}(q)$ if $\frac{1+\pi}{2} \notin \mathrm{End}(E_\jmath)$ and $\mathrm{End}(E_\jmath) \cong \mathcal{O}'(q)$ if $\frac{1+\pi}{2} \in \mathrm{End}(E_\jmath)$ for some q satisfying (2.4.1), and we can identify π and $\pm j$ under this isomorphism. However, q is not unique. By Lemma 1.8 and Proposition 2.1 of [13], one has

Lemma 2.9. *Suppose* $q_1 \neq q_2$ *are primes satisfying* (2.4.1)*. Let* $K = \mathbb{Q}(j) \cong \mathbb{Q}(\sqrt{-p})$*. Suppose* q_1 *and* q_2 *have prime decompositions* $q_1 O_K = \mathfrak{q}_1\bar{\mathfrak{q}}_1$ *and* $q_2 O_K = \mathfrak{q}_2\bar{\mathfrak{q}}_2$*.*

(i) $\mathcal{O}(q_1) \cong \mathcal{O}'(q_2)$ *if and only if* $|\mathcal{O}(q_1)^\times| = |\mathcal{O}'(q_2)^\times| = 4$*. Then* $\mathcal{O}(q_1) \ncong \mathcal{O}'(q_2)$ *if one of them is isomorphic to* $\mathrm{End}(E)$ *for* $\jmath(E) \neq 1728$*.*
(ii) $\mathcal{O}(q_1) \cong \mathcal{O}(q_2) \Leftrightarrow$ *the equation* $x^2 + 4py^2 = q_1q_2$ *is solvable over* $\mathbb{Z} \Leftrightarrow$ *either* $\mathfrak{q}_1\mathfrak{q}_2 \in P_{K,\mathbb{Z}}(2)$ *or* $\mathfrak{q}_1\bar{\mathfrak{q}}_2 \in P_{K,\mathbb{Z}}(2)$*;*
(iii) $\mathcal{O}'(q_1) \cong \mathcal{O}'(q_2) \Leftrightarrow$ *the equation* $x^2 + py^2 = 4q_1q_2$ *is solvable over* $\mathbb{Z} \Leftrightarrow$ *either* $\mathfrak{q}_1\mathfrak{q}_2 \in P_K(2)$ *or* $\mathfrak{q}_1\bar{\mathfrak{q}}_2 \in P_K(2)$*).*

Definition 2.10. For $\jmath \in \mathbb{F}_p$ a supersingular $\jmath$-invariant, set

$$q_\jmath := \min\{q \mid \mathrm{End}(E_\jmath) \cong \mathcal{O}(q) \text{ or } \mathcal{O}'(q)\}.$$

Set

$$M(p) = \max\{q_\jmath \mid \jmath \text{ is a supersingular } \jmath\text{-invariant over } \mathbb{F}_p\}.$$

Certainly $q_0 = 3$ and $q_{1728} = 1$. We shall give the values of $M(p)$ for all primes $p < 2000$ in the appendix.

Example 2.11. Let $p = 101$. We have the following $q_\jmath$ for supersingular $\jmath$-invariant $\jmath$ in $\mathbb{F}_p$:

$$q_{57} = 11,\ q_{59} = 59,\ q_{66} = 67,$$
$$q_{64} = 83,\ q_2 = 139,\ q_{21} = 163.$$

Thus $q_\jmath$ can be bigger than p.

3. Neighborhood of supersingular elliptic curves

In this section we assume that

$$\mathscr{j} \in \mathbb{F}_p \backslash \{0, 1728\} \text{ is a supersingular } \mathscr{j}\text{-invariant}, \ E = E_{\mathscr{j}}, \ \mathrm{End}(E) = \mathcal{O} \text{ and } q = q_{\mathscr{j}}.$$

In this case, then

$$\pi = \pm j, \ \mathcal{O}^\times = \{\pm 1\}, \ R := \mathcal{O} \cap \mathbb{Q}(i) = \begin{cases} \mathbb{Z}[\frac{1+i}{2}], & \text{if } \mathcal{O} = \mathcal{O}(q); \\ \mathbb{Z}[i], & \text{if } \mathcal{O} = \mathcal{O}'(q). \end{cases}$$

Lemma 3.1. *Suppose $\ell \nmid 2pq$. Then in the isogeny graph $\mathscr{G}_\ell(\overline{\mathbb{F}}_\mathrm{p})$,*

(i) *if $\frac{1+\pi}{2} \notin \mathcal{O}$ and $p > q\ell$, then there are $1 + \delta_{-q}$ loops over the vertex $[E]$;*
(ii) *if $\frac{1+\pi}{2} \in \mathcal{O}$ and $p > 4q\ell$, then there are $1 + \delta_{-4q}$ loops over the vertex $[E]$.*

Proof. By Deuring's correspondence theorem, a loop in $\mathscr{G}_\ell(\overline{\mathbb{F}}_\mathrm{p})$ corresponds to a principal left ideal $\mathcal{O}\alpha$ of reduced norm ℓ. If $\frac{1+\pi}{2} \notin \mathcal{O}$, then $\mathcal{O} = \mathcal{O}(q)$. For $\alpha = x + \frac{1+i}{2}y + \frac{j-k}{2}z + \frac{ri-k}{q}w \in \mathcal{O}$, suppose

$$\mathrm{Nrd}(\alpha) = \left(x + \frac{y}{2}\right)^2 + \left(\frac{y}{2} + \frac{rw}{q}\right)^2 q + \left(\frac{z}{2}\right)^2 p + \left(\frac{z}{2} + \frac{w}{q}\right)^2 pq = \ell.$$

If $(z, w) \neq (0, 0)$, then $(\frac{z}{2})^2 + (\frac{z}{2} + \frac{w}{q})^2 q \geq \frac{1}{q}$, and if $p > q\ell$, then $p((\frac{z}{2})^2 + (\frac{z}{2} + \frac{w}{q})^2 q) > \ell$, impossible. Hence $z = w = 0$. Now we need to solve the equation

$$\left(x + \frac{y}{2}\right)^2 + \frac{y^2 q}{4} = \ell \tag{3.0.1}$$

in $\mathbb{Z}$. This is equivalent to the decomposition of the ideal ℓR in the ring $R = \mathcal{O} \cap \mathbb{Q}(i) = \mathbb{Z}[\frac{1+i}{2}]$. Since the discriminant of R is $-q$, by Theorem 2.3, (3.0.1) is solvable over $\mathbb{Z}$ if and only if $\left(\frac{-q}{\ell}\right) = 1$ and $H_{-q}(x)$ splits into linear factors in $\mathbb{F}_\ell[x]$. When this is the case, (3.0.1) has two pairs of solutions up to units in $R^\times = \mathcal{O}^\times = \{\pm 1\}$, corresponding to two different principal left ideals of $\mathcal{O}$ of reduced norm ℓ. Hence there are two loops over $[E]$.

If $\frac{1+\pi}{2} \in \mathcal{O}$, then $\mathcal{O} = \mathcal{O}'(q)$. Suppose $\alpha = x + \frac{1+j}{2}y + iz + \frac{r'i-k}{2q} \in \mathcal{O}$ such that

$$\mathrm{Nrd}(\alpha) = \left(x + \frac{y}{2}\right)^2 + \frac{y^2 p}{4}) + \left(z + \frac{r'w}{2q}\right)^2 q + \frac{pw^2}{4q} = \ell.$$

If $(y, w) \neq (0, 0)$, then $\frac{y^2}{4} + \frac{w^2}{4q} \geq \frac{1}{4q}$, and if $p > 4q\ell$, then $p((\frac{y}{2})^2 + (\frac{w}{2q})^2 q) > \ell$, impossible. Hence $y = w = 0$. Now we need to solve the equation

$$x^2 + z^2 q = \ell \tag{3.0.2}$$

in $\mathbb{Z}$. This is equivalent to the decomposition of ℓR in $R = \mathcal{O} \cap \mathbb{Q}(i) = \mathbb{Z}[i]$. In this case R is of discriminant $-4q$, then by Theorem 2.3, (3.0.2) is solvable over $\mathbb{Z}$ if and only if $\left(\frac{-4q}{\ell}\right) = 1$ and $H_{-4q}(x)$ splits into linear factors in $\mathbb{F}_\ell[x]$. When this is the case, (3.0.2)) has two pairs of solutions up to units in $R^\times = \mathcal{O}^\times$. Thus $\mathcal{O}$ has two principal left ideals of reduced norm ℓ, corresponding to two loops over $[E]$. $\square$

Remark 3.2. We remark that the bounds in Lemma 3.1 are also sharp.

(1) Let $q = 11$, $\ell = 13$. Then $p = 127$ is the largest prime such that $p < q\ell$. Let $E : y^2 = x^3 + 16x + 53$, then E is a supersingular elliptic curve defined over $\mathbb{F}_{127}$ with $\mathrm{End}(E) \cong \mathcal{O}(11)$. By computation, $[E]$ has one loop which is larger than $1 + \delta_{-11} = 0$.

(2) Let $q = 3$, $\ell = 5$. Then $p = 59$ is the largest prime such that $\left(\frac{-p}{q}\right) = 1$ and $p < 4q\ell$. Let $E : y^2 = x^3 + 52x + 15$, then E is supersingular over $\mathbb{F}_{59}$ with $\mathrm{End}(E) \cong \mathcal{O}'(3)$. By computation, $[E]$ has one loop which is larger than $1 + \delta_{-12} = 0$.

Remark 3.3. When the assumption of the above Lemma is satisfied, by the proof above, if $[E]$ has two loops, then the corresponding $\alpha \notin \mathrm{End}(E) \cap \mathbb{Q}(\pi) = \mathcal{O} \cap \mathbb{Q}(j)$. This means the loops are not defined over $\mathbb{F}_p$, since $\mathrm{End}_{\mathbb{F}_p}(E) \subseteq \mathrm{End}(E) \cap \mathbb{Q}(\pi)$.

Proof of Theorem 1.1. If every edge (except loops) in $\mathcal{G}_\ell(\overline{\mathbb{F}}_\mathrm{p})$ has multiplicity one, then the number of vertices adjacent to $[E]$ as predicted by the Theorem is correct. Let X_ℓ be the set of all left $\mathcal{O}$-ideals of reduced norm ℓ. The first part of the Theorem is reduced to show that any non-principal left $\mathcal{O}$-ideal $J \in X_\ell$ of reduced norm ℓ is not equivalent to other ideals in X_ℓ. We prove this by contradiction.

Assume that there exists some $I \in X_\ell - \{J\}$ and $\mu \in B_{p,\infty}^\times$ such that $J = I\mu$, then $\mathrm{Nrd}(\mu) = 1$ and $\ell\mu \in J$.

If $\mathcal{O} = \mathcal{O}(q)$, write $\ell\mu = x + \frac{1+i}{2}y + \frac{j-k}{2}z + \frac{ri-k}{q}w$ in $\mathcal{O}$. Then

$$\mathrm{Nrd}(\ell\mu) = \ell^2 = \left(x + \frac{y}{2}\right)^2 + \left(\frac{y}{2} + \frac{rw}{q}\right)^2 q + \frac{z^2 p}{2} + \left(\frac{z}{2} + \frac{w}{q}\right)^2 pq = \ell^2.$$

If $(z, w) \neq (0, 0)$, then $(\frac{z}{2})^2 + (\frac{z}{2} + \frac{w}{q})^2 q \geq \frac{1}{q}$, and if $p > q\ell^2$, then $p((\frac{z}{2})^2 + (\frac{z}{2} + \frac{w}{q})^2 q) > \ell^2$, impossible. Hence $z = w = 0$. Now we need to solve the equation

$$\left(x + \frac{y}{2}\right)^2 + \frac{qy^2}{4} = \ell^2 \tag{3.0.3}$$

in $\mathbb{Z}$. Note that $(x, y) = (\pm\ell, 0)$ are trivial solutions of (3.0.3). In these cases $\mu = \pm 1$ and $J = I$ which is a contradiction. If there is a nontrivial solution of (3.0.3), then $\ell\mu R = \mathfrak{l}^2$ or $\ell\mu R = \bar{\mathfrak{l}}^2$. Since $q \equiv 3 \bmod 4$, the class number of R is odd, $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ are both principal prime ideals of norm ℓ of R. This implies that $\delta_{-q} = 1$ and $\ell R = \mathfrak{l} \cdot \bar{\mathfrak{l}}$ splits in R. Since $\ell R + (\ell\mu)R \subseteq J$, we have either $\mathfrak{l} \subseteq J$ or $\bar{\mathfrak{l}} \subseteq J$ and hence $J = \mathcal{O}\mathfrak{l}$ or $\mathcal{O}\bar{\mathfrak{l}}$ is a principal left ideal in X_ℓ. This is also a contradiction. The case for $\mathcal{O} = \mathcal{O}'(q)$ can be proved similarly and we omit the proof here.

For the last statement, consider the ℓ-isogenies starting from E, as pointed out in [9, Theorem 2.7], there are exactly $1+\left(\frac{-p}{\ell}\right)$ isogenies defined over $\mathbb{F}_p$, as the loops are not defined over $\mathbb{F}_p$ and the multiplicity of each edge (not including the loops) is one, there are at least $1+\left(\frac{-p}{\ell}\right)$ neighbors of $[E]$ in $\mathscr{G}_\ell(\overline{\mathbb{F}}_{\mathrm{p}})$ defined over $\mathbb{F}_p$. In the following, we will prove that when $p>q\ell^2$ in the first case or $p>4q\ell^2$ in the second case, there are exactly $1+\left(\frac{-p}{\ell}\right)$ neighbors of $[E]$ defined over $\mathbb{F}_p$.

Again we only show the case $\mathcal{O}=\mathcal{O}(q)$. The other case follows by the same argument. For an ideal $I\in X_\ell$, let E_I denote the elliptic curve connecting with E by the isogeny ϕ_I. Then E_I is defined over $\mathbb{F}_p$ if and only if $\mathcal{O}_R(I)\cong\mathrm{End}(E_I)$ contains an element μ such that $\mu^2=-p$ according to Theorem 2.4 and Lemma 2.6. Since $\ell\mathcal{O}\subseteq\mathcal{O}_R(I)\subseteq\frac{1}{\ell}\mathcal{O}$, we may assume $\mu=\frac{1}{\ell}(a+b\frac{1+i}{2}+c\frac{j-k}{2}+d\frac{ri-k}{q})\in\frac{1}{\ell}\mathcal{O}$. By $\mu^2=-p$, then $b=-2a$ and

$$\left(-a+\frac{dr}{q}\right)^2q+\left(\frac{c}{2}\right)^2p+\left(\frac{c}{2}+\frac{d}{q}\right)^2pq=p\ell^2.$$

Thus $p\mid(-aq+dr)$. If $-aq+br\neq0$, when $p>q\ell^2$, then $\frac{(-qa+dr)^2}{q}>p\ell^2$, not possible. Hence $-a+\frac{dr}{q}=0$ and $q\mid d$. Then $\mu=\frac{1}{\ell}(\frac{c}{2}-(\frac{c}{2}+\frac{d}{q})i)j$ with (c,d) satisfying the equation

$$\frac{c^2}{4}+\left(\frac{c}{2}+\frac{d}{q}\right)^2q=\ell^2. \tag{3.0.4}$$

Each solution of (3.0.4) corresponds to a principal ideal in $R=\mathbb{Z}[\frac{1+i}{2}]$ of norm ℓ^2. Since the class number of R is odd when $q\equiv3\bmod4$, $\frac{c}{2}-(\frac{c}{2}+\frac{d}{q})i$ is either $\pm\ell$ or $\pm\alpha^2,\pm\bar{\alpha}^2$ if R has a principal ideal $R\alpha$ of norm ℓ. Thus either $\mu=\pm j$, or when $[E]$ has loops, $\mu=\pm\frac{1}{\ell}\alpha^2j$ or $\pm\frac{1}{\ell}\bar{\alpha}^2j$.

We now follow the notations and ideas in the proof of [14, Theorem 5]. There is a ring isomorphism $\theta:\ \mathcal{O}/\ell\mathcal{O}\to M_2(\mathbb{F}_\ell)$ 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 $\mathbb{F}_\ell$. Let $\iota:\mathcal{O}\to\mathcal{O}/\ell\mathcal{O}$ be the restriction map. The set $\overline{X}_\ell$ of the $\ell+1$ left ideals of $M_2(\mathbb{F}_\ell)$ is

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

where $\omega:=\begin{pmatrix}0&0\\0&1\end{pmatrix}$ and $\omega_a:=\begin{pmatrix}1&a\\0&0\end{pmatrix}$. Under the map $\theta\circ\iota$, there is a 1-to 1 correspondence of X_ℓ and $\overline{X}_\ell$ compatible with multiplication. Thus we only need to check: (i) for which ideal $I\in\overline{X}_\ell$, $I\theta(j)\subseteq I$; (ii) when E has loops, for which ideal $I\in\bar{X}_\ell$, $I\theta(\alpha^2j)\subseteq\ell I=\{0\}$ or $I\theta(\bar{\alpha}^2j)=\{0\}$. Since $\det(\theta(j))=p\neq0$ in $\mathbb{F}_\ell$, to check (ii), it suffices to check: (iii) for which ideal $I\in\bar{X}_\ell$, $I\theta(\alpha^2)\subseteq\ell I=\{0\}$ or $I\theta(\bar{\alpha}^2)=\{0\}$.

When $\left(\frac{-p}{\ell}\right) = 1$, we take $(u, v) = (u, 0)$ where $u^2 = -p \in \mathbb{F}_\ell$. Then $\theta(j) = \begin{pmatrix} u & 0 \\ 0 & -u \end{pmatrix}$. By computation,

$$\omega\theta(j) \in M_2(\mathbb{F}_\ell)\omega,\ \omega_0\theta(j) \in M_2(\mathbb{F}_\ell)\omega_0,\ \omega_a\theta(j) \notin M_2(\mathbb{F}_\ell)\omega_a\ (a \neq 0).$$

Hence there are exactly two ideals $I_1 = \mathscr{O}\ell + \mathscr{O}(u + j)$ and $I_2 = \mathscr{O}\ell + \mathscr{O}(u - j)$ in X_ℓ such that $\pm j \in \mathscr{O}_R(I_1)$ and $\mathscr{O}_R(I_2)$. They correspond to two edges starting from $[E]$ in $\mathscr{G}_\ell(\overline{\mathbb{F}}_{\mathrm{p}})$. If $\left(\frac{-p}{\ell}\right) = -1$, by computation there is no $I \in \bar{X}_\ell$ such that $I\theta(j) \subseteq I$.

When $[E]$ has two loops, let $\alpha = x + \frac{1+i}{2}y \in R$ such that $\alpha\bar{\alpha} = \ell$, then $\ell \nmid y$, and

$$\theta(\alpha^2) = \begin{pmatrix} 2(x + \frac{y}{2})^2 & -(x + \frac{y}{2})yq \\ (x + \frac{y}{2})y & 2(x + \frac{y}{2})^2 \end{pmatrix},\quad \theta(\bar{\alpha}^2) = \begin{pmatrix} 2(x + \frac{y}{2})^2 & (x + \frac{y}{2})yq \\ -(x + \frac{y}{2})y & 2(x + \frac{y}{2})^2 \end{pmatrix}.$$

Let $b = 2\frac{x}{y} + 1$ in $\mathbb{F}_\ell$. Then only

$$\omega_{-b}\theta(\alpha^2) = 0,\ \omega_b\theta(\bar{\alpha}^2) = 0.$$

These two ideals correspond to the principal left ideals $\mathscr{O}\alpha$ and $\mathscr{O}\bar{\alpha}$ in X_ℓ. Thus, except the loops, there are at most two E_I defined over $\mathbb{F}_p$. Since the multiplicity of each edge is one, there are $1 + \left(\frac{-p}{\ell}\right)$ neighbors of $[E]$ in $\mathscr{G}_\ell(\overline{\mathbb{F}}_{\mathrm{p}})$ defined over $\mathbb{F}_p$. $\square$

Example 3.4. Let $p = 311$, $q = 3$, $\ell = 5$. The elliptic curve $E : y^2 = x^3 + 122x + 185$ is supersingular with $\mathrm{End}(E) \cong \mathscr{O}'(3)$. In the 5-isogeny graph $\mathscr{G}_5(\overline{\mathbb{F}}_{311})$, $[E]$ has no loops (as $\left(\frac{-3}{5}\right) = -1$), and only two neighborhoods $\jmath(E_1) = 225$, $\jmath(E_2) = 19$ defined over $\mathbb{F}_{311}$ (as $\left(\frac{-311}{5}\right) = 1$). Moreover $\mathrm{End}(E_1) \cong \mathscr{O}'(67)$ and $\mathrm{End}(E_2) \cong \mathscr{O}'(419)$.

4. The bound of $q_\jmath$ for any supersingular $\jmath$−invariant $\jmath$ in $\mathbb{F}_p$

In this section we identify $K = \mathbb{Q}(\sqrt{-p}) = \mathbb{Q}(j)$ with class number $h = h_K$. Note that

$$O_K = \mathbb{Z}[\sqrt{-p}], \qquad D_K = -4p \quad (\text{if } p \equiv 1 \bmod 4),$$
$$O_K = \mathbb{Z}[\frac{1 + \sqrt{-p}}{2}], \quad D_K = -p \quad (\text{if } p \equiv 3 \bmod 4).$$

Let O be the order of K of conductor 2. Then

$$O = \mathbb{Z} + 2O_K = \begin{cases} \mathbb{Z}[2\sqrt{-p}], & \text{if } p \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{-p}], & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Let L_0 and L_1 be the Hilbert class field and the ring class field of O over K. Then

$$\mathrm{Gal}(L_1/K) \cong \mathrm{cl}(O) \cong I_K(2)/P_{K,\mathbb{Z}}(2),$$

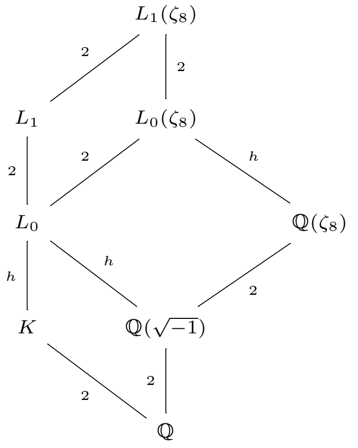

Fig. 1. Field extensions when $p \equiv 1 \bmod 4$.

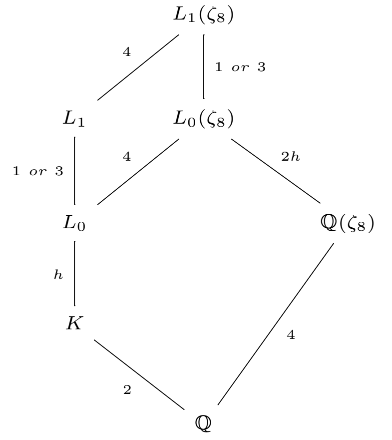

Fig. 2. Field extensions when $p \equiv 3 \bmod 4$.

$$\mathrm{Gal}(L_0/K) \cong \mathrm{cl}(O_K) \cong I_K/P_K \cong I_K(2)/P_K(2).$$

By the inclusion $P_{K,\mathbb{Z}}(2) \subseteq P_K(2)$, $L_1 \supseteq L_0$. Moreover, from [7, Theorem 7.24],

$$[L_1 : L_0] = h(O)/h = \begin{cases} 2, & \text{if } p \equiv 1 \pmod 4, \\ 3, & \text{if } p \equiv 3 \pmod 8, \\ 1, & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

By properties of class fields, we know that $L_0/\mathbb{Q}$ and $L_1/\mathbb{Q}$ are Galois. Let ζ_8 be a primitive eighth root of unity, then $\mathbb{Q}(\zeta_8)$ is a Galois extension of $\mathbb{Q}$. Hence $L_0(\zeta_8)$ and $L_1(\zeta_8)$ are also Galois over $\mathbb{Q}$. By [13, Lemma 2.11], we know that if $p \equiv 3 \bmod 4$, L_0 and $\mathbb{Q}(\zeta_8)$ are linearly disjoint over $\mathbb{Q}$; if $p \equiv 1 \bmod 4$, $L_1 \cap \mathbb{Q}(\zeta_8) = L_0 \cap \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1})$. We have Fig. 1 and 2 about field extensions.

Lemma 4.1. *For $i = 0$ and 1, let $n_i = [L_i(\zeta_8) : \mathbb{Q}]$ and $d_i = |D_{L_i(\zeta_8)}|$.*

(i) *$K(\zeta_8)/\mathbb{Q}$ is an abelian extension of degree 8 and discriminant $2^{16}p^4$.*
(ii) *If $p \equiv 3 \bmod 4$, then $n_0 = 8h$, $d_0 = 2^{16h}p^{4h}$. If furthermore $p \equiv 3 \bmod 8$, then $n_1 = 24h$, $d_1 = 2^{52h}p^{12h}$.*
(iii) *If $p \equiv 1 \bmod 4$, then $n_0 = 4h$, $n_1 = 8h$, $d_0 = 2^{8h}p^{2h}$ and $d_1 \mid 2^{21h}p^{4h}$.*

Proof. For (i), one just needs to compute the discriminant $D_{K(\zeta_8)}$. It is well known $D_{\mathbb{Q}(\zeta_8)} = 2^8$. The extension $K(\zeta_8)/\mathbb{Q}(\zeta_8)$ is unramified outside p and tamely ramified over all primes above p, hence the different $\mathfrak{D}_{K(\zeta_8)/\mathbb{Q}(\zeta_8)} = \prod_{\mathfrak{p}|p \text{ in } \mathbb{Q}(\zeta_8)} \mathfrak{p}^2$ by [15, Theorem 2.6]. By Proposition 2.1(i), we obtain $D_{K(\zeta_8)}$.

The degrees n_0 and n_1 follow from the two figures.

Since L_0 is the Hilbert class field of K which is the maximal unramified abelian extension of K, $D_{L_0/K} = 1$ and by Proposition 2.1(i),

$$D_{L_0} = (D_K)^h.$$

Note that $D_{\mathbb{Q}(\zeta_8)} = 2^8$, $D_{\mathbb{Q}(\sqrt{-1})} = -2^2$. If $p \equiv 3 \bmod 4$, then L_0 and $\mathbb{Q}(\zeta_8)$ are linearly disjoint over $\mathbb{Q}$, and D_{L_0} and $D_{\mathbb{Q}(\zeta_8)}$ are coprime, by Proposition 2.1(ii), then

$$d_0 = D_{L_0(\zeta_8)} = D_{L_0}^{[\mathbb{Q}(\zeta_8):\mathbb{Q}]} \cdot D_{\mathbb{Q}(\zeta_8)}^{[L_0:\mathbb{Q}]} = 2^{16h} \cdot p^{4h}.$$

If $p \equiv 1 \bmod 4$, L_0 and $\mathbb{Q}(\zeta_8)$ are linearly disjoint over $\mathbb{Q}(\sqrt{-1})$. By computation,

$$N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(D_{L_0/\mathbb{Q}(\sqrt{-1})}) = p^h,\ N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(D_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{-1})}) = 2^4.$$

Thus $D_{L_0/\mathbb{Q}(\sqrt{-1})}$ and $D_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{-1})}$ are coprime. By Proposition 2.1(ii), then

$$d_0 = (D_{\mathbb{Q}(\zeta_8)})^h (D_{L_0})^2 (D_{\mathbb{Q}(\sqrt{-1})})^{-2h} = 2^{8h} p^{2h}.$$

To compute d_1, note that L_1/K is ramified only at primes above 2 and L_0/K is unramified, then L_1/L_0 and $L_1(\zeta_8)/L_0$ are ramified only at primes above 2. Note that $L_1/\mathbb{Q}$ is Galois, L_1/L_0 is of degree 2 or 3, all primes of L_0 above 2 must be totally ramified in L_1. We also know 2 is totally ramified in $\mathbb{Q}(\zeta_8)/\mathbb{Q}$. Let e, f and g be the ramification index, the degree of the residue extension and the number of primes above 2 in $L_1(\zeta_8)$. Then $efg = n_{L_1}$ and $2O_{L_1(\zeta_8)}$ has the prime decomposition

$$2O_{L_1(\zeta_8)} = \prod_{i=1}^{g} \mathfrak{P}_{1,i}^e.$$

If $p \equiv 3 \bmod 8$, then primes above 2 are unramified in $L_0/\mathbb{Q}$. We find that $e = 12$, $fg = 2h$ and all primes above 2 in $L_0(\zeta_8)$ are totally (tamely) ramified in $L_1(\zeta_8)$. By [15, Theorem 2.6], we have

$$\mathfrak{D}_{L_1(\zeta_8)/L_0(\zeta_8)} = \prod_{i=1}^{g} \mathfrak{P}_{1,i}^2.$$

Hence

$$d_1 = d_0^3 N_{L_1(\zeta_8)/\mathbb{Q}}(\mathfrak{D}_{L_1(\zeta_8)/L_0(\zeta_8)}) = 2^{52h} p^{12h}.$$

If $p \equiv 1 \bmod 4$, then either $e = 4$ or 8. If $e = 4$, primes above 2 are unramified in $L_1(\zeta_8)/L_0(\zeta_8)$ and the different $\mathfrak{D}_{L_1(\zeta_8)/L_0(\zeta_8)}$ is (1). In this case $d_1 = d_0^2$. If $e = 8$, then

$fg = h$ and primes above 2 are wildly ramified in $L_1(\zeta_8)/L_0(\zeta_8)$. By [15, Theorem 2.6], we have

$$\mathfrak{D}_{L_1(\zeta_8)/L_0(\zeta_8)} = \prod_{i=1}^{g} \mathfrak{P}_{1,i}^{m}, \text{ where } 1 \leq m \leq 5.$$

Hence

$$d_1 = (d_0)^2 N_{L_1(\zeta_8)/\mathbb{Q}}(\mathfrak{D}_{L_1(\zeta_8)/L_0(\zeta_8)}) \mid 2^{21h}p^{4h}. \quad \square$$

Lemma 4.2. *Let q and q' be distinct primes. Let $\sigma_3 = (\zeta_8 \mapsto \zeta_8^3) \in \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$. Then*

(i) *$q \equiv 3 \bmod 8$ and $\left(\frac{q}{p}\right) = -1$ if and only if $[\frac{K(\zeta_8)/\mathbb{Q}}{q}] \in \mathrm{Gal}(K(\zeta_8)/\mathbb{Q})$ is the unique element Δ such that $\Delta|_K = \mathrm{Id}$ and $\Delta|_{\mathbb{Q}(\zeta_8)} = \sigma_3$.*
(ii) *The conditions that q and q' satisfy (2.4.1) and $\mathcal{O}(q) \cong \mathcal{O}(q')$ (resp. $\mathcal{O}'(q) \cong \mathcal{O}'(q')$) is equivalent to that $[\frac{\mathbb{Q}(\zeta_8)/\mathbb{Q}}{q}] = [\frac{\mathbb{Q}(\zeta_8)/\mathbb{Q}}{q'}] = \sigma_3$ and $[\frac{L_1/\mathbb{Q}}{q}] = [\frac{L_1/\mathbb{Q}}{q'}]$ (resp. $[\frac{L_0/\mathbb{Q}}{q}] = [\frac{L_0/\mathbb{Q}}{q'}]$).*

Proof. The condition that $q \equiv 3 \bmod 8$ is equivalent to $[\frac{\mathbb{Q}(\zeta_8/\mathbb{Q}}{q}] = \sigma_3 \in \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$. The condition $(\frac{p}{q}) = -1$ is equivalent to that q splits in K, i.e., $[\frac{K/\mathbb{Q}}{q}] = [\frac{K/\mathbb{Q}}{q'}] = 1$. So (i) holds.

Let $q = \mathfrak{q}\bar{\mathfrak{q}}$ and $q = \mathfrak{q}'\bar{\mathfrak{q}}'$ be the factorization of q and q' in K. By Lemma 2.9(ii), the condition that $\mathcal{O}(q) \cong \mathcal{O}(q')$ is equivalent to

$$\{[\frac{L_1/K}{\mathfrak{q}}], [\frac{L_1/K}{\mathfrak{q}}]^{-1}\} = \{[\frac{L_1/K}{\mathfrak{q}'}], [\frac{L_1/K}{\mathfrak{q}'}]^{-1}\}.$$

Let τ be a lifting of $(\sqrt{-p} \mapsto -\sqrt{-p}) \in \mathrm{Gal}(K/\mathbb{Q})$ in $\mathrm{Gal}(L_1/\mathbb{Q})$ and let $\mathfrak{Q}$ be a prime of L_1 above q, then $[\frac{L_1/\mathbb{Q}}{q}] = \{[\frac{L_1/\mathbb{Q}}{\mathfrak{Q}}], \tau[\frac{L_1/\mathbb{Q}}{\mathfrak{Q}}]\tau^{-1}\}$ (these two probably equal). When $[\frac{K/\mathbb{Q}}{q}] = 1$, this set is equal to $\{[\frac{L_1/K}{\mathfrak{q}}], [\frac{L_1/K}{\mathfrak{q}}]^{-1}\}$. Hence $\mathcal{O}(q) \cong \mathcal{O}(q')$ and $(\frac{p}{q}) = (\frac{p}{q'}) = -1$ is equivalent to

$$[\frac{L_1/\mathbb{Q}}{q}] = [\frac{L_1/\mathbb{Q}}{q'}].$$

The case for $\mathcal{O}'$ follows similarly. $\square$

Lemma 4.3. *Let γ be any element in $\mathrm{Gal}(K(\zeta_8)/\mathbb{Q})$, C_0 and C_1 be any conjugacy class in $\mathrm{Gal}(L_0(\zeta_8)/\mathbb{Q})$ and $\mathrm{Gal}(L_1(\zeta_8)/\mathbb{Q})$ respectively. Assuming GRH.*

(i) *For constant $c > 0$, $\pi_\gamma(c\sqrt{p}, K(\zeta_8)/\mathbb{Q}) \sim \frac{c\sqrt{p}}{4\log p}$ as $p \to \infty$.*

(ii) *Suppose* $p > 2000$ *and* $x \geq p \log^4 p$, *then*

$$\frac{d_0}{|C_0|}\pi_{C_0}(x, L_0(\zeta_8)/\mathbb{Q})\frac{\log x}{\sqrt{x}} \geq \begin{cases} \sqrt{x} - 0.90h\log^2 x, & \textit{if } p \equiv 1 \bmod 4; \\ \sqrt{x} - 1.81h\log^2 x, & \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

$$\frac{d_1}{|C_1|}\pi_{C_1}(x, L_1(\zeta_8)/\mathbb{Q})\frac{\log x}{\sqrt{x}} \geq \begin{cases} \sqrt{x} - 1.88h\log^2 x, & \textit{if } p \equiv 1 \bmod 4; \\ \sqrt{x} - 5.48h\log^2 x, & \textit{if } p \equiv 3 \bmod 8. \end{cases}$$

Suppose $p > 2000$ *and* $x \geq p \log^6 p$, *then*

$$\frac{d_0}{|C_0|}\pi_{C_0}(x, L_0(\zeta_8)/\mathbb{Q})\frac{\log x}{\sqrt{x}} \geq \begin{cases} \sqrt{x} - 0.76h\log^2 x, & \textit{if } p \equiv 1 \bmod 4; \\ \sqrt{x} - 1.51h\log^2 x, & \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

$$\frac{d_1}{|C_1|}\pi_{C_1}(x, L_1(\zeta_8)/\mathbb{Q})\frac{\log x}{\sqrt{x}} \geq \begin{cases} \sqrt{x} - 1.57h\log^2 x, & \textit{if } p \equiv 1 \bmod 4; \\ \sqrt{x} - 4.60h\log^2 x, & \textit{if } p \equiv 3 \bmod 8. \end{cases}$$

Proof. We shall use the explicit formula (2.2.2) in the Chebotarev density Theorem (Theorem 2.2).

For (i), consider the extension $K(\zeta_8)/\mathbb{Q}$, then $d_{K(\zeta_8)} = 2^{16}p^4$ and $n_{K(\zeta_8)} = 8$. Take $x = c\sqrt{p}$, the main term in (2.2.2) is $2c\sqrt{p}/\log p$, the error term is of order $p^{\frac{1}{4}} \log p$. When $p \to \infty$, we get (i).

For (ii), consider the case $L_1/\mathbb{Q}$ and $p \equiv 3 \bmod 8$ case. The other cases can be treated similarly. In this case $n_1 = 24h$ and $d_1 = 2^{52h}p^{12h}$. Note that if $x > 2000$,

$$\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dt}{\log^2 t} \geq \frac{x}{\log x}.$$

By (2.2.2), if $x > 2000$, then

$$\begin{aligned} &\frac{d_1}{|C_1|}\pi_{C_1}(x, L_1(\zeta_8)/\mathbb{Q})\frac{\log x}{\sqrt{x}} \\ \geq &\sqrt{x} - h\log^2 x\left[\frac{36\log p}{\log^2 x} + \frac{156\log 2 + 144}{\log^2 x} + \frac{26\log 2 + 6}{\pi \log x} + \frac{6}{\pi}\frac{\log p}{\log x} + \frac{3}{\pi}\right]. \end{aligned}$$

Note that $\frac{\log p}{\log x} \leq 1$ if $x \geq p$. When p is fixed and $x \geq p\log^4 p$ increases, the other terms inside [ ] of the above inequality decrease; when p increases and $x = p\log^4 p$ or $p\log^6 p$, the other terms inside [ ] also decrease. This leads to the bound in (ii). $\square$

Proof of Theorem 1.3. (1) By the Brauer-Siegel Theorem, the number of supersingular j over $\mathbb{F}_p$ is of order $O(h) = O(\sqrt{p})$, but by Lemma 4.3(i), there are only $O(\frac{\sqrt{p}}{\log p})$ many $q < C\sqrt{p}$ satisfying $q \equiv 3 \bmod 8$ and $(\frac{p}{q}) = -1$ when $p \to \infty$, hence (1) holds.

(2) For $p < 2000$, we check numerically in the appendix that $q_{\jmath} < p\log^2 p$. Suppose $p > 2000$. It suffices to find x such that $\pi_{C_i}(x, L_i(\zeta_8)/\mathbb{Q}) > 0$ for any conjugacy class C_i. By Lemma 4.3(ii), to have $\pi_{C_i}(x, L_i(\zeta_8)/\mathbb{Q}) > 0$, it suffices to find $x \geq p\log^4 p$, such that $\sqrt{x} - Ch\log^2 x > 0$ for different C there. By the Brauer-Siegel Theorem, when p is sufficiently large, $h \sim \sqrt{p}$ if $p \equiv 3 \bmod 4$ or $2\sqrt{p}$ if $p \equiv 1 \bmod 4$. Replace h by $\sqrt{p}$ or $2\sqrt{p}$, we just need to find $x \geq p\log^4 p$, such that $\sqrt{x} - 5.48\sqrt{p}\log^2 x > 0$. This is satisfied if $p > 2000$ and $x = 10000p\log^4 p$.

(3) Suppose $p > 2000$. It suffices to find x such that $\pi_{C_i}(x, L_i(\zeta_8)/\mathbb{Q}) > 0$ for any conjugacy class C_i. By Lemma 4.3(ii), we just need to find $x \geq p\log^6 p$ such that $\sqrt{x} - Ch\log^2 x > 0$ for different C there. By [6, Exercise 5.27], $h < \sqrt{p}\log p$ if $p \equiv 3 \bmod 4$ and $h < \sqrt{4p}\log(4p)$ if $p \equiv 1 \bmod 4$. We thus only need to find $x \geq p\log^6 p$ such that $\sqrt{x} - 4.6\sqrt{p}\log p\log^2 x > 0$. Take $x = 10000p\log^6 p$, we can check $\sqrt{x} - 4.6\sqrt{p}\log p\log^2 x > 0$.

(4) Let q_1, q_2 be two distinct primes satisfying (2.4.1). If (x, y) is an integer solution of $x^2 + 4py^2 = q_1q_2$, y must be even since $q_1q_2 \equiv 1 \bmod 8$ and $x^2 \equiv 0, 1, 4 \bmod 8$. Thus $x^2 + 4py^2 = q_1q_2$ has integer solutions is equivalent to $x^2 + 16py^2 = q_1q_2$ has integer solutions. Thus if both q_1 and $q_2 < 4\sqrt{p}$, the equation has no integer solution and $\mathcal{O}(q_1) \ncong \mathcal{O}(q_2)$ by Lemma 2.9(ii). Similarly by Lemma 2.9(iii), if both q_1 and $q_2 < \frac{\sqrt{p}}{2}$, the equation $x^2 + py^2 = 4q_1q_2$ has no integer solutions, and $\mathcal{O}'(q_1) \ncong \mathcal{O}'(q_2)$. Then if $p \equiv 1 \bmod 4$, $N(4\sqrt{p}) = \pi_\Delta(4\sqrt{p}, K(\zeta_8)/\mathbb{Q})$. If $p \equiv 3 \bmod 4$, $N(\frac{1}{2}\sqrt{p}) = 2\pi_\Delta(\frac{1}{2}\sqrt{p}, K(\zeta_8)/\mathbb{Q})$ and $N(4\sqrt{p}) \geq \pi_\Delta(4\sqrt{p}, K(\zeta_8)/\mathbb{Q}) + \pi_\Delta(\frac{1}{2}\sqrt{p}, K(\zeta_8)/\mathbb{Q})$. $\square$

Appendix A. Comparing $M(p)$ with $\sqrt{p}$ and $p\log^2 p$ when $p < 2000$

For a prime $p > 3$, let $\mathrm{M}(p)$ be the maximal value of $q_{\jmath}$ for all supersingular invariants $\jmath$ over $\mathbb{F}_p$ defined in § 1. The following two tables list the values of $\mathrm{M}(p)$ for all $p < 2000$ and compare it with $\sqrt{p}$ and $p\log^2 p$.

In the following we present our algorithms to compute Table 1 and Table 2. For a finite set A, let $|A|$ denote the cardinality of A.

Algorithm 1
Input: Prime $p \equiv 1 \bmod 4$.
Output: The value $M(p)$.
Procedure:

(1) Compute the set $\mathrm{SSj}(p)$ of all supersingular $\jmath$-invariants in $\mathbb{F}_p$.
(2) Set $\mathrm{SE}(p) =$ the empty set.
(3) For prime $3 \leq q \leq p\log^2 p$ such that $\left(\frac{-p}{q}\right) = 1$ and $q \equiv 3 \bmod 8$, compute the $\jmath$-invariant $\jmath_q \in F_p$ such that $\mathrm{End}(E_{\jmath_q}) \cong \mathcal{O}(q)$. More precisely,
  (3.1) let $v(d)$ be the set of roots of Hilbert class polynomial H_d in $\mathbb{F}_p$. Compute $v(-q)$, $v(-4p)$ and $v(-(\frac{4(r^2+p)}{q}))$.
  (3.2) compute $A = v(-q) \cap v(-4p) \cap v(-(\frac{4(r^2+p)}{q}))$, if $|A| = 1$, return A, otherwise return $A =$ the empty set.

Table 1
The data of prime $p \equiv 1 \bmod 4$.

p	$\mathrm{M}(p)$	$\frac{\mathrm{M}(p)}{\sqrt{p}}$	$\frac{\mathrm{M}(p)}{p \log^2 p}$	p	$\mathrm{M}(p)$	$\frac{\mathrm{M}(p)}{\sqrt{p}}$	$\frac{\mathrm{M}(p)}{p \log^2 p}$	p	$\mathrm{M}(p)$	$\frac{\mathrm{M}(p)}{\sqrt{p}}$	$\frac{\mathrm{M}(p)}{p \log^2 p}$
5	3	1.34	0.232	557	491	20.80	0.022	1193	1483	42.94	0.025
13	11	3.05	0.129	569	4219	176.87	0.184	1201	283	8.17	0.005
17	11	2.67	0.081	577	331	13.78	0.014	1213	619	17.77	0.010
29	19	3.53	0.058	593	587	24.11	0.024	1217	1499	42.97	0.024
37	19	3.12	0.039	601	811	33.08	0.033	1229	1987	56.68	0.0 32
41	211	32.95	0.373	613	307	12.40	0.012	1237	739	21.01	0.012
53	67	9.20	0.080	617	379	15.26	0.015	1249	2003	56.68	0.032
61	59	7.55	0.057	641	1787	70.58	0.067	1277	1499	41.95	0.023
73	43	5.03	0.032	653	491	19.21	0.018	1289	1091	30.39	0.017
89	163	17.28	0.091	661	571	22.21	0.020	1297	179	4.97	0.003
97	59	5.99	0.029	673	107	4.12	0.004	1301	4523	125.40	0.068
101	163	16.22	0.076	677	2203	84.67	0.077	1321	787	21.65	0.012
109	59	5.65	0.025	701	1259	47.55	0.042	1361	4027	109.16	0.057
113	67	6.30	0.027	709	379	14.23	0.012	1373	827	22.32	0.012
137	83	7.09	0.025	733	419	15.48	0.013	1381	691	18.59	0.010
149	619	50.71	0.166	757	379	13.77	0.011	1409	1619	43.13	0.022
157	107	8.54	0.027	761	2003	72.61	0.060	1429	739	19.55	0.010
173	307	23.34	0.067	769	827	29.82	0.024	1433	1907	50.38	0.025
181	163	12.12	0.033	773	547	19.67	0.016	1481	4019	104.43	0.051
193	19	1.37	0.004	797	1987	70.38	0.056	1489	883	22.88	0.011
197	179	12.75	0.033	809	1171	41.17	0.032	1493	947	24.51	0.012
229	179	11.83	0.026	821	1051	36.68	0.028	1549	787	20.00	0.009
233	139	9.11	0.020	829	827	28.72	0.022	1553	1427	36.21	0.017
241	307	19.78	0.042	853	491	16.81	0.013	1597	811	20.29	0.009
257	547	34.12	0.069	857	1627	55.58	0.042	1601	2707	67.65	0.031
269	739	45.06	0.088	877	443	14.96	0.011	1609	1571	39.17	0.018
277	139	8.35	0.016	881	1723	58.05	0.043	1613	2027	50.47	0.023
281	691	41.22	0.077	929	1579	51.81	0.036	1621	811	20.14	0.009
293	691	40.37	0.073	937	659	21.53	0.015	1637	1259	31.12	0.014
313	179	10.12	0.017	941	4603	150.05	0.104	1657	947	23.26	0.010
317	211	11.85	0.020	953	859	27.83	0.019	1669	971	23.77	0.011
337	67	3.65	0.006	977	683	21.85	0.015	1693	971	23.60	0.010
349	499	26.71	0.042	997	571	18.08	0.012	1697	1019	24.74	0.011
353	419	22.30	0.034	1009	571	17.98	0.012	1709	2179	52.71	0.023
373	211	10.93	0.016	1013	827	25.98	0.017	1721	4019	96.88	0.042
389	1051	53.29	0.076	1021	587	18.37	0.012	1733	1451	34.86	0.015
397	227	11.39	0.016	1033	227	7.06	0.005	1741	1019	24.42	0.011
401	251	12.53	0.017	1049	3011	92.97	0.059	1753	1019	24.34	0.010
409	331	16.37	0.022	1061	691	21.21	0.013	1777	1019	24.17	0.010
421	211	10.28	0.014	1069	1579	48.29	0.030	1789	907	21.44	0.009
433	251	12.06	0.016	1093	547	16.55	0.010	1801	859	20.24	0.008
449	659	31.10	0.039	1097	2371	71.59	0.044	1861	4219	97.80	0.040
457	83	3.88	0.005	1109	2851	85.61	0.052	1873	331	7.65	0.003
461	1531	71.31	0.088	1117	563	16.85	0.010	1877	1123	25.92	0.011
509	3923	173.88	0.198	1129	211	6.28	0.004	1889	4523	104.07	0.042
521	2243	98.27	0.110	1153	659	19.41	0.011	1901	3019	69.24	0.028
541	283	12.17	0.013	1181	4019	116.95	0.068	1913	1483	33.91	0.014

(4) Set $\mathrm{SE}(p) = SE(p) \cup A$. Repeat Step 3 until $|\,\mathrm{SE}(p)| = |\,\mathrm{SSj}(p)|$. Return q.

Remark A.1. Recall that when $p \equiv 1 \bmod 4$, for a supersingular elliptic curve E defined over $\mathbb{F}_p$, we have $\mathrm{End}(E) \cong \mathcal{O}(q)$ for some q satisfying

$$\left(\frac{-p}{q}\right) = 1 \text{ and } q \equiv 3 \bmod 8 \tag{A.0.1}$$

Table 2
The data of prime $p \equiv 3 \bmod 4$.

p	$\mathrm{M}(p)$	$\frac{\mathrm{M}(p)}{\sqrt{p}}$	$\frac{\mathrm{M}(p)}{p \log^2 p}$	p	$\mathrm{M}(p)$	$\frac{\mathrm{M}(p)}{\sqrt{p}}$	$\frac{\mathrm{M}(p)}{p \log^2 p}$	p	$\mathrm{M}(p)$	$\frac{\mathrm{M}(p)}{\sqrt{p}}$	$\frac{\mathrm{M}(p)}{p \log^2 p}$
7	3	1.13	0.113	563	1259	53.06	0.056	1291	739	20.57	0.011
11	3	0.90	0.047	571	179	7.49	0.008	1303	227	6.29	0.003
19	11	2.52	0.067	587	419	17.29	0.018	1307	2099	58.06	0.031
23	3	0.63	0.013	599	859	35.10	0.035	1319	1723	47.44	0.025
31	19	3.41	0.052	607	347	14.08	0.014	1327	211	5.79	0.003
43	11	1.68	0.018	619	443	17.81	0.017	1367	811	21.93	0.011
47	59	8.61	0.085	631	163	6.49	0.006	1399	859	22.97	0.012
59	307	39.97	0.313	643	379	14.95	0.014	1423	251	6.65	0.003
67	19	2.32	0.016	647	1163	45.72	0.043	1427	3083	81.61	0.041
71	43	5.10	0.033	659	907	35.33	0.033	1439	1451	38.25	0.019
79	19	2.14	0.013	683	467	17.87	0.016	1447	1163	30.57	0.015
83	131	14.38	0.081	691	419	15.94	0.014	1451	883	23.18	0.011
103	59	5.81	0.027	719	1459	54.41	0.047	1459	1579	41.34	0.020
107	83	8.02	0.036	727	419	15.54	0.013	1471	619	16.14	0.008
127	19	1.69	0.006	739	283	10.41	0.009	1483	1051	27.29	0.013
131	379	33.11	0.122	743	523	19.19	0.016	1487	2339	60.66	0.029
139	107	9.08	0.032	751	163	5.95	0.005	1499	1667	43.06	0.021
151	43	3.50	0.011	787	467	16.65	0.013	1511	1979	50.91	0.024
163	43	3.37	0.010	811	499	17.52	0.014	1523	907	23.24	0.011
167	211	16.33	0.048	823	131	4.57	0.004	1531	3907	99.85	0.047
179	227	16.97	0.047	827	491	17.07	0.013	1543	883	22.48	0.011
191	251	18.16	0.048	839	3467	119.69	0.091	1559	2531	64.10	0.030
199	227	16.09	0.041	859	499	17.03	0.013	1567	907	22.91	0.011
211	59	4.06	0.010	863	547	18.62	0.014	1571	6947	175.27	0.082
223	131	8.77	0.020	883	227	7.64	0.006	1579	563	14.17	0.007
227	139	9.23	0.021	887	971	32.60	0.024	1583	3557	89.40	0.041
239	571	36.93	0.080	907	227	7.54	0.005	1607	1597	39.84	0.018
251	947	59.77	0.124	911	1291	42.77	0.031	1619	2339	58.13	0.026
263	331	20.41	0.041	919	443	14.61	0.010	1627	947	23.48	0.011
271	179	10.87	0.021	947	563	18.30	0.013	1663	331	8.12	0.004
283	163	9.69	0.018	967	139	4.47	0.003	1667	2027	49.65	0.022
307	179	10.22	0.018	971	4051	130.00	0.088	1699	971	23.56	0.010
311	571	32.38	0.056	983	619	19.74	0.013	1723	443	10.67	0.005
331	83	4.56	0.007	991	211	6.70	0.004	1747	443	10.60	0.005
347	251	13.47	0.021	1019	3011	94.32	0.062	1759	691	16.48	0.007
359	467	24.65	0.038	1031	1907	59.39	0.038	1783	1019	24.13	0.010
367	211	11.01	0.016	1039	1307	40.55	0.026	1787	1163	27.51	0.012
379	107	5.50	0.008	1051	283	8.73	0.006	1811	4987	117.19	0.049
383	491	25.09	0.036	1063	883	27.08	0.017	1823	1931	45.23	0.019
419	1427	69.71	0.093	1087	139	4.22	0.003	1831	379	8.86	0.004
431	547	26.35	0.034	1091	3331	100.85	0.062	1847	2003	46.61	0.019
439	307	14.65	0.019	1103	947	28.51	0.017	1867	1091	25.25	0.010
443	331	15.73	0.020	1123	643	19.19	0.012	1871	2803	64.80	0.026
463	67	3.11	0.004	1151	2339	68.94	0.041	1879	2251	51.93	0.021
467	947	43.82	0.054	1163	691	20.26	0.012	1907	2267	51.91	0.021
479	787	35.96	0.043	1171	1163	33.99	0.020	1931	5347	121.68	0.048
487	83	3.76	0.004	1187	947	27.49	0.016	1951	1747	39.55	0.016
491	1187	53.57	0.063	1223	1163	33.26	0.019	1979	3571	80.27	0.031
499	131	5.86	0.007	1231	859	24.48	0.014	1987	1187	26.63	0.010
503	811	36.16	0.042	1259	3347	94.33	0.052	1999	659	14.74	0.006
523	331	14.47	0.016	1279	1019	28.49	0.016				
547	139	5.94	0.006	1283	1051	29.34	0.016				

Here we do a loop for q satisfying (A.0.1) in an ascending order, and compute the corresponding j-invariant j, then make them into a set. In this way, if in some step, we get the equality $\mathrm{SE}(p) = \mathrm{SSj}(p)$, then we get the maximal q_j.

One thing needed to explain is the following: in Step 3, we compute the associated supersingular $\mathscr{j}$-invariant $\mathscr{j}_q$ of q by computing the common roots of H_{-q}, H_{-4p} and $H_{-(\frac{4(r^2+p)}{q})}$ in $\mathbb{F}_p$. Since by [5, Theorem 3], $\mathscr{j}_q$ is a root of H_{-d} if and only if $\mathscr{O}^T(q) = \mathbb{Z}\langle i, j-k, \frac{2(ri-k)}{q}\rangle$ has an element of reduced norm d. This is the case since $i, 2j, \frac{ri-k}{2} \in \mathscr{O}^T(q)$ are of reduced norm $q, 4p$ and $\frac{4(r^2+p)}{q}$ respectively. Thus if $v(-q) \cap v(-4p) \cap v(-(\frac{4(r^2+p)}{q}))$ has just one element, it must be $\mathscr{j}_q$. If it has more than one element, we quit this q and do Step 3 for the next q. Thus the output of algorithm 1 is equal or larger than the real $\mathrm{M}(p)$. But in our experiment, we find the intersection of these three sets always has one element. Anyway, the data in Table 1 and Table 2 is enough to show that $\mathrm{M}(p) < p\log^2 p$.

Algorithm 2
Input: Prime $p \equiv 3 \bmod 4$.
Output: The value $M(p)$.
Procedure:

(1) Compute the set $\mathrm{SSj}(p)$ of all supersingular $mathrsfsj$-invariants with $\mathscr{j} \in \mathbb{F}_p \setminus \{1728\}$.
(2) Set $\mathrm{SE}(p)$ and $\mathrm{XE}(p)$ to be the empty sets.
(3) For all prime $3 \le q \le p\log^2 p$ such that $\left(\frac{-p}{q}\right) = 1$ and $q \equiv 3 \bmod 8$, do
  (3.1) compute the $\mathscr{j}$-invariant $\mathscr{j}_q \in \mathbb{F}_p$ such that $\mathrm{End}(E_{\mathscr{j}_q}) \cong \mathscr{O}(q)$ as in Algorithm 1. If $\mathscr{j}_q \neq 1728$, set $\mathrm{SE}(p) = \mathrm{SE}(p) \cup \{\mathscr{j}_q\}$, otherwise, set $\mathrm{SE}(p) = \mathrm{SE}(p) \cup \emptyset$.
  (3.2) compute the prime ideal decomposition of q in $K = \mathbb{Q}(\sqrt{-p})$: $(q) = \mathfrak{q}_1\mathfrak{q}_2$. If $\mathfrak{q}_1$ is not principal, set $\mathrm{XE}(p) = \mathrm{XE}(p) \cup \{[\mathfrak{q}_1], [\mathfrak{q}_2]\}$ where $[\mathfrak{q}_1]$ and $[\mathfrak{q}_2]$ are the ideal classes in the class group of K. Otherwise, set $\mathrm{XE}(p) = \mathrm{XE}(p) \cup \emptyset$.
(4) Compare $|\mathrm{SSj}(p)|$ and $|\mathrm{SE}(p)| + \frac{|\mathrm{XE}(p)|}{2}$. If they are equal, return q. Otherwise repeat Step 3.

Remark A.2. When $p \equiv 3 \bmod 4$, for a supersingular elliptic curve E defined over $\mathbb{F}_p$, we have $\mathrm{End}(E) \cong \mathscr{O}(q)$ or $\mathscr{O}'(q)$ for some q satisfying (A.0.1), and for $\mathscr{j} \neq 1728$, $\mathscr{O}(q) \ncong \mathscr{O}'(q)$ by Lemma 2.9(i). Here, we do a loop for q satisfying (A.0.1) in an ascending order. First we compute the $\mathscr{j}-$invariant $\mathscr{j}_q$ such that $\mathrm{End}(E_{\mathscr{j}_q}) \cong \mathscr{O}(q)$ for each q as in algorithm 1. For the $\mathscr{j}$-invariant of $\mathscr{O}'(q)$, if we compute the other three Hilbert class polynomials as in the case of $\mathscr{O}(q)$, the running time is very expensive, thus we use another way. We define a set $\mathrm{XE}(p)$ consisting of ideal classes $[\mathfrak{q}_1]$ and $[\mathfrak{q}_2]$ if they are not equal, and each correspond to one supersingular $\mathscr{j}$-invariant $\mathscr{j}'$ such that $\mathrm{End}(E_{\mathscr{j}'}) \cong \mathscr{O}'(q)$, if $[\mathfrak{q}_1] = [\mathfrak{q}_2] = 1$, they correspond to $\mathscr{j} = 1728$ by Lemma 2.9(iii). Thus when $|\mathrm{SSj}(p)| = |\mathrm{SE}(p,r)| + \frac{|\mathrm{XE}(p,r)|}{2}$, we obtain the maximal $q_{\mathscr{j}}$.

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.-M. Couveignes, Hard homogeneous spaces, IACR Cryptology ePrint Archive 2006/291, https://ia.cr/2006/291, 2006.
[3] D.X. Charles, K.E. Lauter, E.Z. Goren, Cryptographic hash functions from expander graphs, J. Cryptol. 22 (2009) 93–113.
[4] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, CSIDH: an efficient post-quantum commutative group action, IACR Cryptology ePrint Archive 2018/383.
[5] I. Chevyrev, S. Galbraith, Constructing supersingular elliptic curves with a given endomorphism ring, LMS J. Comput. Math. 17 (suppl. A) (2014) 71–91.
[6] H. Cohen, A Course in Computational Algebraic Number Theory, GTM, vol. 138, Springer, 1996.
[7] D.A. Cox, Primes of the Form $x^2 + ny^2$, second edition, John Wiley & Sons, 2013.
[8] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hansischen Univ. 14 (1941) 197–272.
[9] C. Delfs, S. Galbraith, Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$, Des. Codes Cryptogr. 78 (2016) 425–440.
[10] L. De Feo, D. Jao, J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, J. Math. Cryptol. 8 (2014) 209–247.
[11] L. Grenié, G. Molteni, An explicit Chebotarev density theorem under GRH, J. Number Theory 200 (2019) 441–485.
[12] S. Galbraith, C. Petit, J. Silva, Identification protocols and signature schemes based on supersingular isogeny problems, in: Advances in Cryptology – ASIACRYPT 2017, Springer, 2017, pp. 3–33.
[13] T. Ibukiyama, On maximal orders of division quaternion algebra over the rational number field with certain optimal embeddings, Nagoya Math. J. 88 (1982) 181–195.
[14] S. Li, Y. Ouyang, Z. Xu, Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728, Finite Fields Appl. (January 2020), https://doi.org/10.1016/j.ffa.2019.101600.
[15] J. Neukirch, Algebraic Number Theory, Springer-Verlag, Berlin, 1999.
[16] Y. Ouyang, Z. Xu, Loops of isogeny graphs of supersingular elliptic curves at $j = 0$, Finite Fields Appl. 58 (2019) 174–176.
[17] A.K. Pizer, Ramanujan graphs and Hecke operators, Bull. Am. Math. Soc. (N.S.) 23 (1) (1990) 127–137.
[18] A. Rostovtsev, A. Stolbunov, Public-key cryptosystem based on isogenies, Cryptology ePrint Archive, Report 2006/145, 2006, http://eprint.iacr.org/.
[19] J.H. Silverman, The Arithmetic of Elliptic Curves, GTM, vol. 106, Springer, New York, 2009.
[20] A. Sutherland, Elliptic curves lecture 21, https://math.mit.edu/classes/18.783/2019/lectures.html.
[21] J. Voight, Quaternion algebras, v.0.9.15, May 26, 2019, https://www.math.dartmouth.edu/jvoight/quat.html.