SUPERSINGULAR PRIMES FOR ELLIPTIC CURVES OVER $\mathbb{Q}$

MAKOTO SUWAMA

1. Introduction

This is a note on Noam Elkies' paper [7] on the existence of infinitely many supersingular primes for elliptic curves over $\mathbb{Q}$.

Throughout this note, for E/k and E'/k elliptic curves, and $\overline{k}$ an algebraic closure of k, define

$$\mathrm{Hom}(E, E') := \mathrm{Hom}_{\overline{k}}(E, E') \qquad \text{and} \qquad \mathrm{End}(E) := \mathrm{Hom}(E, E).$$

And take k to be a perfect field (may not be necessary).

2. Supersingular Elliptic Curves

In this section we define supersingularity.

Theorem 2.1 (Deuring '41 [5]). *Let E/k be an elliptic curve with k a field with characteristic $p > 0$. Then the following are equivalent:*

(1) $E[p^r](\overline{k}) = 0$ *for one (all)* $r \geq 1$.
(2) $\widehat{F}_r$ *is (purely) inseparable for one (all)* $r \geq 1$, *where* $\widehat{F}_r$ *is the dual of the* p^r*th-power Frobenius map.*
(3) *The map* $[p] : E \to E$ *is purely inseparable and* $j(E) \in \mathbb{F}_{p^2}$.
(4) $\mathrm{End}(E)$ *is an order in a quaternion algebra.*

Proof. See Theorem V.3.1 in [13]. □

Definition 2.2 If E has the properties given in Theorem 2.1, then it is called *supersingular*. Otherwise we say E is *ordinary*.

We also have another useful characterisation for supersingular elliptic curves if they are defined over a finite field.

Proposition 2.3. *Let $q = p^r$ with p a prime, and $E/\mathbb{F}_q$ an elliptic curve. If $F : E \to E$ is the q-th power Frobenius map, then E is supersingular if and only if*

$$\mathrm{tr}(F) \equiv 0 \pmod{p}.$$

Moreover, if $p > 3$, then $E/\mathbb{F}_p$ is supersingular if and only if

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

Proof. We have $[\mathrm{tr}(F)] = F + \widehat{F}$, so

$$\widehat{F} = [\mathrm{tr}(F)] - F.$$

Now from Corollary III.5.5 in [13], for $m, n \in \mathbb{Z}$, $[m] + nF$ is separable if and only if $p \nmid m$. Hence $\widehat{F}$ is separable if and only if $p \nmid \operatorname{tr}(F)$. So E is supersingular if and only if $p \mid \operatorname{tr}(F)$.

For the second part, if $p > 3$, then by the Hasse bound, we have

$$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p} < p.$$

Now,

$$\operatorname{tr}(F) = 1 + \deg(F) - \deg(1 - F),$$

with $\deg(F) = p$ and $\deg(1 - F) = \#E(\mathbb{F}_p)$, so

$$|\operatorname{tr}(F)| = |1 + p - \#E(\mathbb{F}_p)| < p.$$

And so $p \mid \operatorname{tr}(F)$ if and only if $\operatorname{tr}(F) = 0$. □

Remark 2.4 For $p > 3$, the number of supersingular elliptic curve over $\mathbb{F}_{p^2}$ (up to $\overline{F}_{p^2}$-isomorphism) is

$$\#\left\{E/\mathbb{F}_{p^2} \mid E \text{ is supersingular}\right\} = \begin{cases} \lfloor \frac{p}{12} \rfloor + 2 & \text{if } p \equiv 11 \pmod{12} \, \{j = 0, 1728\} \\ \lfloor \frac{p}{12} \rfloor + 1 & \text{if } p \equiv 7 \pmod{12} \, \{j = 1728\} \\ \lfloor \frac{p}{12} \rfloor + 1 & \text{if } p \equiv 5 \pmod{12} \, \{j = 0\} \\ \lfloor \frac{p}{12} \rfloor & \text{if } p \equiv 1 \pmod{12} \end{cases}$$

For $p = 3$, there is only 1 supersingular elliptic curve. See Theorem V.4.1 in [13]. If we restrict to $E/\mathbb{F}_p$, then we have

$$\#\left\{E/\mathbb{F}_p \mid E \text{ is supersingular}\right\} = \begin{cases} 2^{-1}h & \text{if } p \equiv 1 \pmod{4} \\ 2h & \text{if } p \equiv 3 \pmod{8} \\ h & \text{if } p \equiv 7 \pmod{8} \end{cases}$$

where $h = h(\mathbb{Q}(\sqrt{-p}))$ is the class number[1].

Remark 2.5 One of the most important application of supersingular elliptic curve is cryptography. Given a large prime p and a small prime ℓ, *supersingular isogeny graph* is a graph where the nodes are the j-invariants of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, and the edges are degree ℓ-isogenies. The key here is that since all supersingular elliptic curves are isogenous, the graph is connected and admits other nice properties. There are key exchange, signature schemes and public-key cryptography based on the graph, and as of 2018, there are no known sub-exponential time algorithms for breaking these schemes, even on quantum computers[6].

Definition 2.6 For K a number field, an elliptic curve E/K and a prime of good reduction $\mathfrak{p}$ of K, we say that $\mathfrak{p}$ is a *supersingular prime* for E if the reduction of E modulo $\mathfrak{p}$ is supersingular. Otherwise $\mathfrak{p}$ is called an *ordinary prime* for E.

Remark 2.7 Distinction between supersingular primes and ordinary primes are important in Iwasawa theory of elliptic curves. They are treated differently, and the supersingular case is much harder[14].

Question 2.8 Given an elliptic curve E/K, what can you say about

$$S(E/K) := \{p \mid p \text{ is a supersingular prime for } E/K\}?$$

Answers to the above question:

(1) (Deuring '41[5]) If E is a CM elliptic curve, then $S(E/\mathbb{Q})$ has a density $\frac{1}{2}$ amongst all primes. (His result generalises to arbitrary number field and not just over $\mathbb{Q}$. See Theorem 2.10).
(2) (Elkies '87 [7]) $S(E/\mathbb{Q})$ is infinite for any $E/\mathbb{Q}$ (or any number field K with $[K:\mathbb{Q}]$ is odd.)
(3) (Elkies '89 [8]) $S(E/K)$ is infinite for any E/K if K is a real number field.
(4) (Jao '05 [9]) $S(E/K)$ is infinite for elliptic curves satisfying certain conditions about cyclic p-isogeny.
(5) (Lang-Trotter '76 [11]) Conjectured that if $E/\mathbb{Q}$ is without CM, then the asymptotic is $\frac{c\sqrt{x}}{\log x}$. (Some progress has been made[4], but it is open as of 2018).

We have the following main lemma for proving supersingularity that are used in both of Elkies' paper, and also in Jao's paper.

Lemma 2.9. *Let E/k be an elliptic curve with $\operatorname{char} k = p > 0$. Then E is supersingular if there exist an order $\mathcal{O}$ of an imaginary quadratic field K such that $\mathcal{O} \subset \operatorname{End}(E)$ and p does not split in K.*

Proof. We will prove the contrapositive, so suppose E is ordinary. Then either $\operatorname{End}(E)$ is isomorphic to $\mathbb{Z}$ or an imaginary quadratic order $\mathcal{O}$. If it is $\mathbb{Z}$, then E cannot be CM by any $\mathcal{O}$, so we are done. If it is isomorphic to $\mathcal{O}$, then tensoring the p-adic representation

$$\operatorname{End}(E) \otimes \mathbb{Z}_p \to \operatorname{End}_{\mathbb{Z}_p}(T_p(E))$$

with $\mathbb{Q}$, we get

$$K \otimes \mathbb{Q}_p \to \mathbb{Q}_p.$$

But the left hand side is a 2-dimensional $\mathbb{Q}_p$-algebra, so the map has a kernel. Hence the tensor product is not a field and so p splits in K. □

For a CM elliptic curve over a number field, Deuring have proven a nice characterisation of a supersingular prime.

Theorem 2.10 (Deuring, '41 [5]). *Let E be an elliptic curve over a number field F with CM by $\mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic field K. Let $\mathfrak{P}$ be a prime of F of good reduction for E lying above p. Then $\mathfrak{P}$ is an ordinary prime if and only if p splits in K.*

Proof. See Theorem 13.12 in [10]. □

3. Hilbert Class Polynomials

Given $E/\mathbb{Q}$, by Lemma 2.9 the question now becomes, how to find a prime p such that $\operatorname{End}(E_p)$ contains a suitable order. We will be using the Hilbert class polynomial to find p such that $\operatorname{End}(E_p)$ contains $\mathcal{O}$.

Definition 3.1 Given an imaginary quadratic order $\mathcal{O}$, define

$$\operatorname{Ell}_{\mathcal{O}}(\mathbb{C}) = \{E/\mathbb{C} \mid \operatorname{End}(E) \cong \mathcal{O}\}/\text{isomorphisms}$$

Definition 3.2 Given $D \in \mathbb{Z}$ such that $D > 0$ and $D \equiv 0, 3 \pmod 4$, define

$$\mathcal{O}_D := \mathbb{Z}\left[\frac{D + \sqrt{-D}}{2}\right]$$

an order of $\mathbb{Q}(\sqrt{-D})$ with discriminant $-D$.

Lemma 3.3. *Suppose $\ell \equiv 3 \pmod 4$ is a prime. Then for $D = \ell$ or 4ℓ, $h(\mathcal{O}_D)$ is odd.*

Proof. See Proposition 3.11 and Theorem 7.7(ii) in [3]. $\square$

Definition 3.4 Suppose $D \in \mathbb{Z}$ such that $D > 0$ and $D \equiv 0, 3 \pmod 4$. Then the *Hilbert class polynomial of discriminant $-D$* is

$$H_D(X) := H_{\mathcal{O}_D}(X) := \prod_{E \in \mathrm{Ell}_{\mathcal{O}_D}(\mathbb{C})} (X - j(E))$$

Remark 3.5 Some authors use the term *Hilbert class polynomial* when $\mathcal{O}_D$ is a maximal order, and use the term *ring class polynomial* for the general case, since the splitting field of $H_{\mathcal{O}}(X)$ is the ring class field of $\mathcal{O}$. See Theorem 11.1 in [3].

Proposition 3.6. *$H_D(X) \in \mathbb{Z}[X]$ and is irreducible over $K = \mathbb{Q}(\sqrt{-D})$.*

Proof. See Corollary 21.13 and Theorem 21.14 in [15]. $\square$

Lemma 3.7. *Let K_D be splitting field of $H_D(X)$ over $K = \mathbb{Q}(\sqrt{-D})$. Then $K_D/\mathbb{Q}$ is Galois, and*

$$\mathrm{Gal}(K_D/\mathbb{Q}) \cong \mathrm{Gal}(K_D/K) \rtimes (\mathbb{Z}/2\mathbb{Z}).$$

where the non-trivial element of $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(K_D/K)$ by sending σ to its inverse σ^{-1}.

Proof. See Lemma 9.3 in [3]. $\square$

Corollary 3.8. *We have the following diagram of fields:*

$$\begin{tikzcd}
& & & K_D = \mathbb{Q}(\sqrt{-D}, x_1) \arrow[dlll, dash] \arrow[dll, dash] \arrow[d, dash] \arrow[ddr, dash] & \\
\mathbb{Q}(x_1) \arrow[ddrrr, dash] & \mathbb{Q}(x_2) \arrow[ddrr, dash] & \dots & \mathbb{Q}(x_n) \arrow[dd, dash] & \\
& & & & K = \mathbb{Q}(\sqrt{-D}) \arrow[dl, dash] \\
& & & \mathbb{Q} &
\end{tikzcd}$$

where x_i's are roots of $H_D(X)$. Moreover, $\mathbb{Q}(x_i)$'s are distinct fields.

Proof. Follows from the structure of the Galois group $\mathrm{Gal}(K_D/\mathbb{Q})$. $\square$

Here onwards, let ℓ be a prime 3 mod 4.

Theorem 3.9 (Deuring's Lifting Theorem [5]). *Let $E_0/\overline{\mathbb{F}}_p$ be an elliptic curve, and let $\alpha_0 \in \mathrm{End}(E_0)$ be a non-trivial endomorphism. Then there exist an elliptic curve $E/\mathcal{O}_K$ for K a number field, an endomorphism $\alpha \in \mathrm{End}(E)$ and a prime $\mathfrak{p}$ of K lying above p with residue field k, such that*

$$E_k \cong_{\overline{F}_p} E_0 \quad \textit{and} \quad \alpha_{\overline{F}_p} = \alpha_0.$$

Proof. We will prove the case assuming E_0 is ordinary. Theorem 1.7.4.5 in [2] has a proof for supersingular case, although it will lift it to local field as opposed to a number field. Suppose $p \mid \deg(\alpha_0)$. Then

$$p \nmid \deg(\alpha_0 + [m]) = \deg(\alpha_0) + m\mathrm{tr}(\alpha_0) + m^2$$

for some $m \in \mathbb{Z}$, and since we can lift $[m]$, we may assume $p \nmid \deg(\alpha_0)$. Now suppose $\ker \alpha_0$ is not cyclic. Then

$$\ker[m] \subset \ker \alpha_0$$

for some $m \in \mathbb{Z}$, so there exist $\beta_0 \in \mathrm{End}(E_0)$ such that $\alpha_0 = \beta_0 \circ [m]$. Once again, we can always lift $[m]$, so we may assume $\ker \alpha_0$ is cyclic.

Let $n = \deg(\alpha_0)$ and

$$E_0'/\mathbb{Q}(t) : y^2 + (t - 1728)xy = x^3 - 36(t - 1728)^3 x - (t - 1728)^5$$

an elliptic curve with a j-invariant t and a discriminant $t^2(t - 1728)^9$. Let $Z_1, \dots, Z_s$ be the cyclic order n subgroups of E_0'. Then for $i = 1, \dots, s$, we have isogenies

$$\lambda_i : E_0' \to E_i' := E_0'/Z_i$$

defined over $\mathbb{Q}(t, E_0'[n])$. Let j_i be the j-invariant of E_i' and let R be the integral closure of $\mathbb{Z}[t, j_1, \dots, j_s, E_0'[n]] \subset \mathbb{Q}(t, j_1, \dots, j_s, E_0'[n])$. Now consider the map

$$r : \mathbb{Z}[t] \to \overline{\mathbb{F}}_p, t \mapsto j(E_0).$$

Since R is integral over $\mathbb{Z}[t]$, the map extends to

$$r : R \to \overline{\mathbb{F}}_p$$

Let $\mathfrak{m} = \ker r$. Now E_0 is ordinary, so $j(E_0) \neq 0, 1728$ and hence $\mathfrak{m} \not\ni \Delta(E_0) = t^2(t - 1728)^9$. Therefore for each $i = 0, \dots, s$, we can pick a model $\mathcal{E}_i/R$ of E_i' such that it has a good reduction at $\mathfrak{m}$. If $k(\mathfrak{m}) := R/\mathfrak{m}$, then

$$E_0 \cong_{\overline{k}} (\mathcal{E}_0)_{k(\mathfrak{m})}$$

since their j-invariants are the same. Moreover $p \nmid n$, so $E_0'[n] \hookrightarrow (\mathcal{E}_0)_k \cong E_0$ and hence $Z_i \hookrightarrow E_0[n]$ for $i = 1, \dots, s$. Now by counting the cyclic order n subgroup of $E_0[n]$, we see that one of the Z_i must be equal to $\ker \alpha_0$. So without loss of generality, suppose $(Z_1)_k = \ker \alpha_0$.

$$\begin{tikzcd} E_0 \arrow[r, "\alpha_0"] \arrow[dr, "\lambda_{1,k(\mathfrak{m})}"] & E_0 \arrow[d, leftrightarrow, "\cong"] \\ & (\mathcal{E}_1)_{k(\mathfrak{m})} \end{tikzcd}$$

so $(\mathcal{E}_0)_{k(\mathfrak{m})} \cong (\mathcal{E}_1)_{k(\mathfrak{m})}$, and hence $\mathfrak{q} := (t - j_1) \subset \mathfrak{m}$. Let $S := R/\mathfrak{q}$ and K be the fraction field of S, and let

$$E := (\mathcal{E}_0)_S \quad \text{and} \quad E_1 := (\mathcal{E}_1)_S.$$

Now S is integral over $\mathbb{Z}$, so K is a number field. And now $j(E) = j(E_1)$, so after some finite degree base extension of K, we have $E \cong E_1$. Hence we can consider

$$\lambda_{1,S} : E \to E_1 \in \mathrm{End}(E) \qquad \text{with } \ker \lambda_{1,S} = (Z_1)_S.$$

So we have an elliptic curve E/S, with $S = \mathcal{O}_K$ and K a number field, with a prime $\mathfrak{p} = \mathfrak{m}/\mathfrak{q}$ lying above p with residue field k satisfying:

$$j(E_k) = j((\mathcal{E}_0)_k) = j(E_0), \text{ so } E_k \cong_{\overline{\mathbb{F}}_p} E_0$$

and

$$\alpha := \lambda_{1,S} \in \mathrm{End}(E) \quad \text{with} \quad \ker \alpha_{\overline{F}_p} = \ker \alpha_0.$$

Now since E_0 is ordinary, $\mathrm{Aut}(\mathrm{End}(E_0)) = \{\pm 1\}$, so α_k and α_0 may differ by $[-1]$, but in which case we will take $-\alpha$ instead of α and we will have $\alpha_k = \alpha_0$. $\square$

Lemma 3.10. *Let $E_1, E_2 \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, and let $\mathfrak{a}_i \subset \mathcal{O}$ be ideals such that $E_i \cong \mathbb{C}/\mathfrak{a}_i$. Then as $\mathcal{O}$-modules,*

$$\mathrm{Hom}(E_1, E_2) \cong J$$

for any ideal J in the same ideal class as $\mathfrak{a}_1^{-1}\mathfrak{a}_2$. Moreover, for $\alpha \in J$,

$$\deg(\alpha) = \frac{\mathrm{N}_{\mathcal{O}}(\alpha)}{\mathrm{N}(J)}.$$

Proof.

$$\begin{aligned}
\mathrm{Hom}(\mathbb{C}/\mathfrak{a}_1, \mathbb{C}/\mathfrak{a}_2) &= \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a}_1 \subset \mathfrak{a}_2\} \\
&= \{\alpha \in K \mid \alpha\mathfrak{a}_1 \subset \mathfrak{a}_2\} \\
&= \mathfrak{a}_1^{-1}\mathfrak{a}_2.
\end{aligned}$$

And for $\alpha \in \mathfrak{a}_1^{-1}\mathfrak{a}_2$,

$$\begin{aligned}
\deg(\alpha) &= (\mathfrak{a}_2 : \alpha\mathfrak{a}_1) \\
&= (\mathcal{O} : \alpha)(\alpha : \alpha\mathfrak{a}_1)(\mathcal{O} : \mathfrak{a}_2)^{-1} \\
&= \mathrm{N}_{\mathcal{O}}(\alpha)\,\mathrm{N}(\mathfrak{a}_1)\,\mathrm{N}(\mathfrak{a}_2)^{-1} \\
&= \frac{\mathrm{N}_{\mathcal{O}}(\alpha)}{\mathrm{N}(\mathfrak{a}_1^{-1}\mathfrak{a}_2)}
\end{aligned}$$

$\square$

Proposition 3.11. *Let K be a number field, $\mathfrak{p}$ a prime of K, E_1/K and E_2/K elliptic curves with good reduction at $\mathfrak{p}$, and $\overline{E}_1$ and $\overline{E}_2$ their reduction modulo $\mathfrak{p}$. Let L/K be a finite extension such that $\mathrm{Hom}_L(E_1, E_2) = \mathrm{Hom}(E_1, E_2)$, and let $\mathfrak{P}$ a prime of L lying above $\mathfrak{p}$. Then the natural reduction map*

$$\mathrm{Hom}_L(E_1, E_2) \to \mathrm{Hom}(\overline{E}_1, \overline{E}_2)$$

is degree preserving injection.

Proof. See Proposition II.4.4 in [12]. ∎

Lemma 3.12. $H_\ell(12^3) = H_{4\ell}(12^3) = 0 \pmod{\ell}$.

Proof. Consider an elliptic curve $E_\ell/\mathbb{F}_\ell$ given by $y^2 = x^3 - x$. There exists an automorphism

$$I : E_\ell \to E_\ell, (x, y) \mapsto (-x, \sqrt{-1}y).$$

And $I^2 = -1$, so $\mathbb{Z}[I]$ is an imaginary quadratic order with $\mathbb{Z}[I] \subset \mathrm{End}(E_\ell)$. Now $\ell \equiv 3 \pmod 4$, so ℓ does not split in $\mathbb{Q}(I)$ and so E_ℓ is supersingular by Lemma 2.9. If $\ell > 3$, then by Proposition 2.3, the Frobenius F satisfies $\mathrm{tr}(F) = 0$. If $\ell = 3$, then $\#E_\ell(\mathbb{F}_3) = 4$, so $\mathrm{tr}(F) = 0$ in this case as well. Hence

$$0 = F^2 - \mathrm{tr}(F)F + \deg(F) = F^2 + \ell.$$

Moreover, since all 2-torsions are $\mathbb{F}_\ell$-rational, $\ker([2]) \subset E_\ell(\mathbb{F}_\ell) = \ker(1 - F)$, and so

$$\tfrac{1-F}{2} \in \mathrm{End}(E_\ell).$$

Hence

$$\mathrm{End}(E_\ell) \supset \mathbb{Z} \oplus \mathbb{Z}I \oplus \mathbb{Z}\tfrac{1+F}{2} \oplus \mathbb{Z}\tfrac{I+IF}{2}$$

with $I^2 = -1$, $F^2 = -\ell$ and $IF = -FI$. The order on the right-hand side has discriminant ℓ, so it is maximal (see 15.1 in [16]), hence

$$\mathrm{End}(E_\ell) = \mathbb{Z} \oplus \mathbb{Z}I \oplus \mathbb{Z}\tfrac{1+F}{2} \oplus \mathbb{Z}\tfrac{I+IF}{2}.$$

Now by Theorem 3.9, we can lift E_ℓ and $\frac{1+F}{2}$ to E/K and $\alpha \in \mathrm{End}(E)$ so that E and α reduces to E_ℓ and $\frac{1+F}{2}$ respectively modulo some prime $\mathfrak{l}$ of K above ℓ. Now $\mathbb{Z}[\alpha] \cong \mathbb{Z}[\frac{1+\sqrt{-\ell}}{2}] = \mathcal{O}_\ell$ is the ring of integers of $\mathbb{Q}(\sqrt{-\ell}) \cong \mathrm{End}(E) \otimes \mathbb{Q}$, so $\mathrm{End}(E) = \mathbb{Z}[\alpha]$. And $j(E_\ell) = 1728$, so we have $E \in \mathrm{Ell}_{\mathcal{O}_\ell}(\mathbb{C})$ with $j(E) \equiv 1728 \pmod{\mathfrak{l}}$. Hence

$$H_\ell(12^3) \equiv 0 \pmod{\ell}.$$

Similarly, we can lift E_ℓ and IF to obtain E/K with $\beta \in \mathrm{End}(E)$ with $\mathrm{End}(E) \supset \mathbb{Z}[\beta] \cong \mathcal{O}_{4\ell}$. And $\frac{1+\beta}{2} \notin \mathrm{End}(E)$, because $\frac{1+IF}{2} \notin \mathrm{End}(E_\ell)$. Hence $\mathrm{End}(E) = \mathbb{Z}[\beta]$ and $E \in \mathrm{Ell}_{\mathcal{O}_{4\ell}}(\mathbb{C})$, so

$$H_{4\ell}(12^3) \equiv 0 \pmod{\ell}.$$

∎

Lemma 3.13. *Let $D = \ell$ or 4ℓ, K_D be the splitting field of $H_D(X)$ over $K := \mathbb{Q}(\sqrt{-\ell})$ and let x_0 be a root of $H_D(X)$. Then there exists a unique prime $\mathfrak{l}$ of K_D lying above ℓ, such that $x_0 \equiv 12^3 \pmod{\mathfrak{l}}$.*

Proof. Existence of $\mathfrak{l}$ is proven by Lemma 3.12. Suppose there exist another prime $\mathfrak{l}'$ lying above ℓ such that $x_0 \equiv 12^3 \pmod{\mathfrak{l}'}$. Then there exist $\sigma \in \mathrm{Gal}(K_D/\mathbb{Q})$ such that $\sigma(\mathfrak{l}') = \mathfrak{l}$. Then

$$x_1 := \sigma(x_0)$$

is another root of $H_D(X)$ and since $x_0 \equiv 12^3 \pmod{\mathfrak{l}'}$, we have

$$x_1 = \sigma(x_0) \equiv 12^3 \pmod{\sigma(\mathfrak{l}') = \mathfrak{l}}.$$

So we have $x_0 \equiv 12^3 \equiv x_1 \pmod{\mathfrak{l}}$. Let E_0 and E_1 be distinct elliptic curves with j-invariant x_0 and x_1, both of which reduces to E_ℓ mod $\mathfrak{l}$ (E_ℓ is from the previous lemma). Hence we obtain a degree-preserving embedding

$$\phi : \mathrm{Hom}(E_0, E_1) \hookrightarrow \mathrm{End}(E_\ell) =: A.$$

Now by Lemma 3.10, we have $\mathrm{Hom}(E_0, E_1) \cong J \subset \mathcal{O}_D$ for some non-principal ideal J, and for $x \in \mathrm{Hom}(E_0, E_1)$, $\deg(x) = \mathrm{N}_{\mathcal{O}_D}(x)/\,\mathrm{N}(J)$. Let $\alpha, \beta \in J$ be a $\mathbb{Z}$-basis of J, and define

$$q(x,y) = \frac{\mathrm{N}_{\mathcal{O}_D}(\alpha x + \beta y)}{\mathrm{N}(J)},$$

a quadratic form on J. Now for $x \in \mathrm{End}(E_\ell)$, $\deg(x) = \mathrm{N}_A(x)$, so we have a map

$$\phi : J \to \operatorname{im}\phi \subset A$$

that respects the quadratic form $q(x,y)$. Now to show that E_0 and E_1 cannot be distinct, we will treat $D = \ell$ and $D = 4\ell$ cases separately and show that they both lead to contradiction.

Case 1. $D = \ell$: Now by Theorem 2.8 in [3], we can change the basis so that it is reduced, i.e.

$$q(x,y) = ax^2 + bxy + cy^2$$

with $|b| \le a \le c$. Moreover, the discriminant $D = b^2 - 4ac = -\ell$, and so $a \le \sqrt{\frac{-D}{3}} = \sqrt{\frac{\ell}{3}}$. And now,

$$c = \frac{b^2+\ell}{4a} \le \frac{1}{4}\left(a + \frac{\ell}{a}\right) \le \frac{1+\ell}{4}.$$

But if $c = \frac{1+\ell}{4}$, then $q(x,y) = x^2 - x + \frac{1+\ell}{4}$ which corresponds to the trivial ideal class in $Cl(\mathcal{O}_\ell)$ and J is not principal so that is not possible. Hence we have $c < \frac{1+\ell}{4}$, and J admits a $\mathbb{Z}$-basis α_1, α_2 such that

$$\deg(\alpha_j) < \frac{1+\ell}{4} \qquad \text{for } j = 1, 2.$$

Now if $\alpha_j = a_j + b_j I + c_j \frac{1+F}{2} + d_j \frac{I+IF}{2} \in R$ with $a_j, b_j, c_j, d_j \in \mathbb{Z}$, then

$$\begin{aligned}
q(x,y) &= \mathrm{N}_A(\alpha_1 x + \alpha_2 y) \\
&= \mathrm{N}_A\left((a_1x + a_2y) + (b_1x + b_2y)I + (c_1x + c_2y)\tfrac{1+F}{2} + (d_1x + d_2y)\tfrac{I+IF}{2}\right) \\
&= \left(\left(a_1 + \tfrac{c_1}{2}\right)^2 + \left(b_1 + \tfrac{d_1}{2}\right)^2 + \tfrac{\ell}{4}\left(c_1^2 + d_1^2\right)\right)x^2 \\
&\quad + \left(2a_1a_2 + 2b_1b_2 + 2c_1c_2\tfrac{1+\ell}{4} + 2d_1d_2\tfrac{1+\ell}{4} + a_1c_2 + a_2c_1 + b_1d_2 + b_2d_1\right)xy \qquad (1) \\
&\quad + \left(\left(a_2 + \tfrac{c_2}{2}\right)^2 + \left(b_2 + \tfrac{d_2}{2}\right)^2 + \tfrac{\ell}{4}\left(c_2^2 + d_2^2\right)\right)y^2
\end{aligned}$$

so in particular,

$$\deg(\alpha_j) = \left(a_j + \tfrac{c_j}{2}\right)^2 + \left(b_j + \tfrac{d_j}{2}\right)^2 + \tfrac{\ell}{4}\left(c_j^2 + d_j^2\right)$$

And now $\deg(\alpha_j) < \frac{1+\ell}{4}$ implies $c_j = 0 = d_j$, and hence $\operatorname{im}\phi \subset \mathbb{Z}[I]$. But the fundamental volume of J is

$$\operatorname{vol}(J) = \sqrt{\frac{-D}{4}} = \frac{\sqrt{\ell}}{2},$$

and every sub-lattice of $\mathbb{Z}[I]$ has integral fundamental volume so it is a contradiction. Hence E_0 and E_1 cannot be distinct so x_0 is the unique root with $x_0 \equiv 12^3 \pmod{\mathfrak{l}}$.

Case 2. $D = 4\ell$. Now by Theorem 2.8 in [3], we can change the basis so that it is reduced, i.e.

$$q(x, y) = ax^2 + bxy + cy^2$$

with $|b| \leq a \leq c$. Moreover, the discriminant $D = b^2 - 4ac = -4\ell$, and so $a \leq \sqrt{\frac{-D}{3}} = \sqrt{\frac{4\ell}{3}}$. And now,

$$c = \frac{b^2 + 4\ell}{4a} \leq \frac{1}{4}\left(a + 4\frac{\ell}{a}\right) \leq \frac{1 + 4\ell}{4}.$$

But $c \in \mathbb{Z}$, so $c \leq \ell$, and if $c = \ell$, then $q(x, y) = x^2 + \ell$ which corresponds to the trivial ideal class in $Cl(\mathcal{O}_{4\ell})$ and J is not principal so that is a contradiction. Hence we have $c < \ell$. Now if $c < \frac{1+\ell}{4}$, then the proof for case 1 will show that $\operatorname{im}\phi \subset \mathbb{Z}[I]$, and will lead to a contradiction since $\operatorname{vol}(J) = \sqrt{\ell}$. So we are going to assume $\frac{1+\ell}{4} \leq c < \ell$. Moreover since $-4\ell = D = b^2 - 4ac$, we have $2|b$, so the restrictions are:

$$2 \leq |b| \leq a \leq c \quad \text{and} \quad \tfrac{1+\ell}{4} \leq c < \ell.$$

If $a = 2$, then $|b| = 2$ and $c = \frac{1+\ell}{2}$. But then $q(x, y)$ is primitive (see Theorem 7.7 in [3]) so this is not possible.

If $a = 3$, then $|b| = 2$ and $c = \frac{1+\ell}{3}$. Now from $a \leq c$, we have $\ell \geq 8$, and also $3 \mid 1 + \ell$, so $\ell \geq 11$. Now if $\alpha_j = a_j + b_j I + c_j \frac{1+F}{2} + d_j \frac{I+IF}{2}$ is the $\mathbb{Z}$-basis of $\operatorname{im}\phi$ with $\deg(\alpha_1) = a = 3$ and $\deg(\alpha_2) = c = \frac{1+\ell}{3}$, then by considering eq. (1), we must have

$$\left(a_1 + \tfrac{c_1}{2}\right)^2 + \left(b_1 + \tfrac{d_1}{2}\right)^2 + \tfrac{\ell}{4}\left(c_1^2 + d_1^2\right) = 3. \tag{2}$$

If $\ell = 11$, then without loss of generality, we can assume $a_1 = b_1 = d_1 = 0$ and $c_1 = 1$. Moreover $c = 3$ so $a_2 = b_2 = 0$ and either $c_2 = \pm 1$ or $d_2 = \pm 1$. But by looking at $b = \pm 2$, we have

$$6c_2 + a_2 = b = \pm 2,$$

and this is not possible. If $\ell > 11$, then $\frac{1+\ell}{4} > 3$, and so from eq. (2), we have $c_1 = 0 = d_1$. But $a_1^2 + b_1^2 = 3$ has no solution, so this also not possible. Hence $a = 3$ is not possible.

If $a = 4$, then either $|b| = 2$ or $|b| = 4$. If $|b| = 4$, then $c = \frac{16+4\ell}{16}$ which is not possible since $c \in \mathbb{Z}$. So $|b| = 2$ and $c = \frac{1+\ell}{4}$. From $a \leq c$, we have $4 \leq c = \frac{1+\ell}{4}$ so $15 \leq \ell$, but ℓ is a prime so $17 \leq \ell$. Hence $\frac{\ell}{4} > 4$ and from

$$\left(a_1 + \tfrac{c_1}{2}\right)^2 + \left(b_1 + \tfrac{d_1}{2}\right)^2 + \tfrac{\ell}{4}\left(c_1^2 + d_1^2\right) = a = 4,$$

we have $c_1 = 0 = d_1$, and either $a_1^2 = 4$ or $b_1^2 = 4$. So without loss of generality, assume $a_1 = 2$. Then by looking at $b = \pm 2$, we have

$$4a_2 + c_2 = b = \pm 2.$$

and so $2|c_2$. But

$$\left(a_2 + \tfrac{c_2}{2}\right)^2 + \left(b_2 + \tfrac{d_2}{2}\right)^2 + \tfrac{\ell}{4}\left(c_2^2 + d_2^2\right) = c = \tfrac{1+\ell}{4}$$

so $c_2 = 0$ and we get $4a_2 = \pm 2$ a contradiction. So $a = 4$ is also not possible.

If $a \geq 5$ then

$$\tfrac{1+\ell}{4} \leq c = \tfrac{b^2+4\ell}{4a} \leq \tfrac{1}{4}\left(a + 4\tfrac{\ell}{a}\right) \leq \tfrac{1}{4}\left(5 + \tfrac{4}{5}\ell\right),$$

which implies $\ell \leq 19$. But $5 \leq a \leq \sqrt{\frac{4\ell}{3}}$, so in fact $\ell = 19$ and $a = 5$. And $|b| = 2$ or 4, but since $c = \frac{b^2+4\ell}{4a}$, $|b| = 2$. Hence $c = 16$. You can check that there is no integer solutions to

$$\begin{aligned}
\left(a_1 + \tfrac{c_1}{2}\right)^2 + \left(b_1 + \tfrac{d_1}{2}\right)^2 + \tfrac{19}{4}\left(c_1^2 + d_1^2\right) &= 5\\
2a_1a_2 + 2b_1b_2 + 10c_1c_2 + 10d_1d_2 + a_1c_2 + a_2c_1 + b_1d_2 + b_2d_1 &= \pm 2\\
\left(a_2 + \tfrac{c_2}{2}\right)^2 + \left(b_2 + \tfrac{d_2}{2}\right)^2 + \tfrac{19}{4}\left(c_2^2 + d_2^2\right) &= 16
\end{aligned}$$

which proves that $D = 4\ell$ case is also not possible, and hence x_0 is the unique root with $x_0 \equiv 12^3 \pmod{\mathfrak{l}}$.

□

Proposition 3.14. *For $D = \ell$ or 4ℓ, there exists $R(X) \in \mathbb{F}_\ell[X]$ such that*

$$H_D(X) \equiv (X - 12^3)R(X)^2 (\text{mod } \ell)$$

Proof. Let x_0, K_D and $\mathfrak{l}$ be as in Lemma 3.13. From Corollary 3.8, we know there exists an involution in $\sigma \in \mathrm{Gal}(K_D/\mathbb{Q})$ such that $\sigma(x_0) = x_0$. And from Lemma 3.13, we know that σ also fixes $\mathfrak{l}$, so we can reduce σ mod $\mathfrak{l}$. Now the Galois group of the residue fields $\mathrm{Gal}(k(\mathfrak{l}), \mathbb{F}_\ell)$ is also a subquotient of $\mathrm{Gal}(K_D/K)$ since the inertia degree of $\sqrt{-\ell}/\ell$ is 1. And $\mathrm{Gal}(K_D/K) \cong Cl(\mathcal{O}_D)$ is odd by Lemma 3.3, so the involution must be trivial on the residue field. Moreover, by Corollary 3.8, σ does not fix any other roots, so $\sigma(x) \equiv x \pmod{\mathfrak{l}}$ for any $x \neq x_0$ a root of $H_D(X)$. Hence

$$H_D(X) \equiv (X - 12^3)R(X)^2 \pmod{\ell}$$

for some $R(X) \in \mathbb{F}_\ell[X]$. □

Lemma 3.15. *The only real roots of $H_\ell(X)$ and $H_{4\ell}(X)$ are $j(\frac{1}{2}(1 + \sqrt{-\ell}))$ and $j(\sqrt{-\ell})$ respectively.*

Proof. From the bijection between the ideal class group of $\mathcal{O}_D$ and $\mathrm{Ell}_{\mathcal{O}_D}(\mathbb{C})$, we see that the complex conjugation acting on the roots of $H_D(X)$ corresponds to complex conjugation on the ideal class. Now,

$$I\bar{I} = N(I)\mathcal{O}_D \implies \bar{I} = I^{-1} \in Cl(\mathcal{O}_D),$$

so the ideal classes fixed by the complex conjugations are the 2-torsion of the class group. But for $D = \ell$ or 4ℓ, $Cl(\mathcal{O}_D)$ is odd by Lemma 3.3, so there is only one class fixed by the conjugation in each class group. Hence the only real roots are the ones corresponding to the trivial classes in $Cl(\mathcal{O}_D)$.

Finally the j-invariants corresponding to $\mathcal{O}_\ell$ and $\mathcal{O}_{4\ell}$ are $j(\frac{1}{2}(1+\sqrt{-\ell}))$ and $j(\sqrt{-\ell})$ respectively. $\square$

Lemma 3.16. *For all $J \in \mathbb{R}$, there exist $L_J > 0$ such that for all $\ell > L_J$, $H_\ell(J) > 0$ and $H_{4\ell}(J) < 0$.*

Proof. Since $j_\ell = j(\frac{1}{2}(1+\sqrt{-\ell}))$ and $j_{4\ell} = j(\sqrt{-\ell})$ are the only real roots, it suffices to show that $j_\ell \to -\infty$ and $j_{4\ell} \to \infty$ as $\ell \to \infty$. And from

$$j(\tau) = \tfrac{1}{q} + 744 + 196884q + \dots, \qquad \text{where } q = \exp(2\pi i\tau)$$

we see that as $\ell \to \infty$, $j_\ell \to -\infty$ and $j_{4\ell} \to \infty$. So for sufficiently large ℓ, $j_\ell < J$ and $j_{4\ell} > J$. $\square$

4. Supersingular primes

Theorem 4.1 (Elkies '87 [7])**.** *Let S be a finite set of primes. Then $E/\mathbb{Q}$ has a supersingular prime outside S.*

Proof. Without loss of generality, we can assume that S contains all the primes of bad reduction for E. Now let ℓ be a prime satisfying the following conditions:

(1) $\left(\frac{p}{\ell}\right) = 1$ for all $p \in S$,
(2) $\left(\frac{-1}{\ell}\right) = -1$, and
(3) $\ell > L_{j(E)}$, where $L_{j(E)}$ is from Lemma 3.16.

The first two conditions are congruence conditions, so by Dirichlet's theorem on primes in arithmetic progression, there exist infinitely many primes satisfying those conditions above.

Now suppose there exist a prime p satisfying the conditions below:

(1) $p \mid M$ where $H_\ell(j(E))H_{4\ell}(j(E)) =: -\frac{M}{N}$, where $M, N > 0$, and
(2) $\left(\frac{p}{\ell}\right) = -1$ or $p = \ell$.

Note that $H_\ell(j(E))H_{4\ell}(j(E)) < 0$ by Lemma 3.16 and by our choice of ℓ. Then there exist E'/K_ℓ with CM by $\mathcal{O}_D$ and a prime $\mathfrak{p}$ of K_ℓ above p such that

$$j(E) \equiv j(E') \bmod \mathfrak{p}.$$

Hence after reduction modulo $\mathfrak{p}$,

$$\mathrm{End}(E_p) \cong \mathrm{End}(E'_\mathfrak{p}) \supset \mathcal{O}_D.$$

And since $\left(\frac{p}{\ell}\right) = -1$ or $p = \ell$, p does not split in $K = \mathbb{Q}(\sqrt{-\ell})$, and so p is a supersingular prime of E. Moreover, condition (1) on ℓ and condition (2) on p implies $p \notin S$.

Now it remains to show that such p exists. So suppose no such p exists. Then every prime dividing M is a quadratic residue mod ℓ, so $\left(\frac{M}{\ell}\right) = 1$. And $H_\ell(X)H_{4\ell}(X)$ has an even degree, so N is a square and hence $\left(\frac{N}{\ell}\right) = 1$. Now, from Proposition 3.14,

$$-\frac{M}{N} = (j(E) - 12^3)^2 R(j(E))^2 Q(j(E))^2 \pmod{\ell},$$

but that is a contradiction since $\left(\frac{-1}{\ell}\right) = -1$ by the construction of ℓ. Hence p satisfying above conditions exists. $\square$

Remark 4.2 The proof of Theorem 4.1 holds for elliptic curves E defined over a number field L if $[L : \mathbb{Q}]$ is odd. The main differences are as follows:

- If S is a finite set of primes of L, then take $S_{\mathbb{Q}} = \{\mathfrak{p} \cap \mathbb{Z} \mid \mathfrak{p} \in S\}$.
- Look at the prime factors of $\mathrm{N}_{L/\mathbb{Q}}(H_\ell(j(E))H_{4\ell}(j(E)))$, and since $[L : \mathbb{Q}]$ is odd, the norm will be negative for sufficiently large ℓ.

We then find p and then pick a prime $\mathfrak{p}$ of L above p such that $\mathrm{End}(E_{\mathfrak{p}}) \supset \mathcal{O}_D$, and that will show $\mathfrak{p}$ is a supersingular prime.

References

[1] Centeleghe, T. G. On supersingular elliptic curves over $\mathbf{F_p}$. preprint on webpage at `https://wwwproxy.iwr.uni-heidelberg.de/groups/arith-geom/centeleghe/up.pdf`, last visited on 2019/1/20. 2

[2] Chai, C.-L., Conrad, B., and Oort, F. *Complex multiplication and lifting problems*, vol. 195 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2014. 5

[3] Cox, D. A. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. 4, 8, 9

[4] David, C., and Pappalardi, F. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, 4 (1999), 165–183. 3

[5] Deuring, M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ. 14* (1941), 197–272. 1, 3, 5

[6] Eisenträger, K., Hallgren, S., Lauter, K., Morrison, T., and Petit, C. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in cryptology—EUROCRYPT 2018. Part III*, vol. 10822 of *Lecture Notes in Comput. Sci.* Springer, Cham, 2018, pp. 329–368. 2

[7] Elkies, N. D. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math. 89*, 3 (1987), 561–567. 1, 3, 11

[8] Elkies, N. D. Supersingular primes for elliptic curves over real number fields. *Compositio Math. 72*, 2 (1989), 165–172. 3

[9] Jao, D. Supersingular primes for points on $X_0(p)/w_p$. *J. Number Theory 113*, 2 (2005), 208–225. 3

[10] Lang, S. *Elliptic functions*, second ed., vol. 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1987. With an appendix by J. Tate. 3

[11] Lang, S., and Trotter, H. *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers. 3

[12] Silverman, J. H. *Advanced topics in the arithmetic of elliptic curves*, vol. 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. 7

[13] Silverman, J. H. *The arithmetic of elliptic curves*, second ed., vol. 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2009. 1, 2

[14] Sprung, F. E. I. Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures. *J. Number Theory 132*, 7 (2012), 1483–1506. 2

[15] Sutherland, A. Mit mathematics 18.783, lecture notes: Elliptic curves, 2017. URL: `https://math.mit.edu/classes/18.783/2017/lectures.html`. Last visited on 2019/01/16. 4

[16] Voight, J. Quaternion algebras, 2018. URL: `https://math.dartmouth.edu/~jvoight/quat-book.pdf`. Last visited on 2019/01/16. 7