Functiones et Approximatio
60.1 (2019), 41–59
doi: 10.7169/facm/1655

ON SUPERSINGULAR PRIMES OF THE ELKIES' ELLIPTIC CURVE

Naoki Murabayashi

Abstract: Let E be the elliptic curve $y^2 = x^3 + (i-2)x^2 + x$ over the imaginary quadratic field $\mathbb{Q}(i)$. In this paper, we investigate the supersingular primes of E. We introduce the curve C of genus two over $\mathbb{Q}$ covering a quotient of E and for any prime number p, we state a condition (over $\mathbb{F}_p$) about the reduction of the jacobian variety of C modulo p which is equivalent to the existence of a supersingular prime of E lying over p (Theorem 5.10).

Keywords: curve of genus two, quadratic twist, supersingular abelian surface, ideal class, Magma, Groebner basis.

1. Introduction

In [2] Elkies proved that for any number field K of odd degree over $\mathbb{Q}$, every elliptic curve defined over K has infinitely many supersingular primes. He remarked that for number fields of even degree over $\mathbb{Q}$, the situation is more complicated. As examples, he also presented the elliptic curve

$$E : y^2 = x^3 + (i-2)x^2 + x$$

defined over $\mathbb{Q}(i)$ $(i^2 = -1)$, to which his method for existence of infinitely many supersingular primes does not apply. He showed that an odd supersingular characteristic p of E must be inert in $\mathbb{Q}(i)$ (i.e., $p \equiv 3 \pmod 4$) and the number of supersingular primes (p) of E with $p \leqslant x$ is expected to behave as $C \cdot \log\log x$ for some constant C when x tends to infinity. He also stated that a computer search found no odd supersingular prime less than 74000. Since the prime ideal $(1+i)$ is a bad prime of E, this means that E has no supersingular prime whose characteristic of the residue field is less than 74000.

Using Magma [1], the author obtained that E has no supersingular prime whose characteristic of the residue field is less than 5×10^{10}. The program is very simple:

This research was financially supported by the Kansai University Grant-in-Aid for progress of research in graduate course, 2016−2018.

2010 Mathematics Subject Classification: primary: 11G20; secondary: 11Y50

```
for t in [m..n] do
   if IsPrime(3+4*t) then
      F:=FiniteField(3+4*t);
      PF<x>:=PolynomialAlgebra(F);
      F2<a>:=ext<F|x^2+4*x+5>;
      E:=EllipticCurve([0,a,0,1,0]);
      if IsSupersingular(E) then
         print 3+4*t;
      end if;
   end if;
end for;
```

where m and n in the first line are non-negative specified integers with m < n. We executed this program at intervals 125×10^5 with respect to t for prime numbers less than 7×10^8. For other prime numbers, intervals with respect to t were the following.

prime number p	interval with respect to t
$7 \times 10^8 \leqslant p < 9 \times 10^8$	250×10^5
$9 \times 10^8 \leqslant p < 42 \times 10^8$	500×10^5
$42 \times 10^8 \leqslant p < 70 \times 10^8$	1000×10^5
$70 \times 10^8 \leqslant p < 15 \times 10^9$	2000×10^5
$15 \times 10^9 \leqslant p < 5 \times 10^{10}$	2500×10^5

One of the reasons why supersingular primes of E are rare is that for any supersingular prime (p), the reduction of E modulo (p) has no model defined over $\mathbb{F}_p$.

In this paper we construct a curve C of genus two defined over $\mathbb{Q}$ whose jacobian variety $J(C)$ is isogenous to $E \times E^\sigma$ over $\mathbb{Q}(i)$ ($\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \langle\sigma\rangle$) and investigate properties over $\mathbb{F}_p$ of the reduction of $J(C)$ modulo p for any supersingular prime (p) of E.

2. A curve of genus two covering a quotient of *E*

Let C be the curve

$$y^2 = x^5 + 16x^4 - 8x^3 - 64x^2 + 16x \ (= x(x-2)(x+2)(x^2+16x-4)\,)$$

of genus two defined over $\mathbb{Q}$. Set $P := (0,\,0) \in E[2]$, the set of 2-torsion points of E and $E_1 := E/\langle P\rangle$. Then it is straightforward to check that E_1 is defined by an equation

$$y^2 = x(x+4)(x+i)$$

and

$$\varphi : C \longrightarrow E_1, \qquad (x,\,y) \longmapsto \left(\frac{x}{4} - \frac{1}{x},\, \frac{1}{8x}\left(1 + \frac{2i}{x}\right) y\right)$$

is a morphism of degree two. Therefore C has the automorphism

$$\eta : C \longrightarrow C, \qquad (x,\, y) \longmapsto \left(-\frac{4}{x},\, -8i\frac{y}{x^3}\right)$$

which is the generator of the Galois group of φ. Putting

$$\psi := \varphi \times \varphi^{\sigma} : C \longrightarrow E_1 \times E_1^{\sigma},$$

we consider the isogeny

$$\Phi : J(C) \longrightarrow E_1 \times E_1^{\sigma}, \qquad cl(P_1 + P_2 - 2\infty) \longmapsto \psi(P_1) + \psi(P_2),$$

where ∞ denotes the unique Weierstrass point of C at infinity and $cl(P_1+P_2-2\infty)$ denotes the linearly equivalent class represented by a divisor $P_1 + P_2 - 2\infty$ of C. Let R_1, R_2, R_3, R_4, R_5 and R_6 be the Weierstrass points of C whose x-coordinates are infinity, 0, -2, 2, $-8-2\sqrt{17}$ and $-8+2\sqrt{17}$, respectively (therefore, $R_1 = \infty$).

Theorem 2.1. *The kernel of* Φ *is*

$$\{0, cl(R_2 - R_1), cl(R_4 - R_3), cl(R_6 - R_5)\}$$

and isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$.

Proof. We take any element $cl(P_1+P_2-2\infty)$ of $J(C)$. Under the assumption that $P_1 \in \{R_1,\ R_2\}$, $cl(P_1 + P_2 - 2\infty) \in \operatorname{Ker}\Phi$ is equivalent to $P_2 \in \{R_1,\ R_2\}$ because of the fact that $\varphi^{-1}(O) = \{R_1,\ R_2\}$, where O is the point at infinity of E_1. In this case we have two elements 0 and $cl(R_1+R_2-2\infty) = cl(R_2-R_1)$ of $\operatorname{Ker}\Phi$. Therefore it is enough to consider the case $P_j \notin \{R_1,\ R_2\}$ $(j = 1,\ 2)$. Then considering the coordinate $(x_j,\ y_j)$ of P_j $(j = 1,\ 2)$, we have that $cl(P_1 + P_2 - 2\infty) \in \operatorname{Ker}\Phi$ if and only if

$$\frac{1}{4}x_1 - \frac{1}{x_1} = \frac{1}{4}x_2 - \frac{1}{x_2}, \tag{2.1}$$

$$\frac{1}{8x_1}\left(1 + \frac{2i}{x_1}\right) y_1 = -\frac{1}{8x_2}\left(1 + \frac{2i}{x_2}\right) y_2, \tag{2.2}$$

$$\frac{1}{8x_1}\left(1 - \frac{2i}{x_1}\right) y_1 = -\frac{1}{8x_2}\left(1 - \frac{2i}{x_2}\right) y_2. \tag{2.3}$$

It follows that (2.1) is equivalent to

$$\frac{1}{4}(x_1 - x_2) = -\frac{x_1 - x_2}{x_1 x_2}.$$

It is divided into two cases: $x_1 - x_2 \neq 0$ and $x_1 - x_2 = 0$.

In the former case, we have that $x_2 = -\frac{4}{x_1}$. By substituting this for (2.2) and (2.3), we have that

$$\frac{1}{x_1}\left(1 + \frac{2i}{x_1}\right) y_1 = \frac{1}{4}x_1\left(1 - \frac{i}{2}x_1\right) y_2, \tag{2.4}$$

$$\frac{1}{x_1}\left(1 - \frac{2i}{x_1}\right) y_1 = \frac{1}{4}x_1\left(1 + \frac{i}{2}x_1\right) y_2. \tag{2.5}$$

If $x_1 = 2i$ (resp. $-2i$), $x_2 = -\frac{4}{x_1} = 2i$ (resp. $-2i$). Hence we have that $x_1 = x_2$, so a contradiction. Therefore we obtain that $x_1 \neq \pm 2i$. If $y_1 \neq 0$ and $y_2 \neq 0$, dividing both sides of (2.4) by both sides of (2.5), we obtain that

$$\left(1+\frac{2i}{x_1}\right)\left(1+\frac{i}{2}x_1\right) = \left(1-\frac{2i}{x_1}\right)\left(1-\frac{i}{2}x_1\right)$$

and this implies $x_1 = \pm 2i$, so a contradiction. We consider the case: $y_1 = 0$. If $y_2 \neq 0$, (2.4) implies $x_1 = -2i$. This is a contradiction. We have that $y_2 = 0$. Therefore x_1 and x_2 are roots of the equation $x(x+2)(x-2)(x^2+16x-4) = 0$ whose product equals to -4. Hence we have that $\{P_1,\ P_2\} = \{R_3,\ R_4\}$ or $\{R_5,\ R_6\}$, i.e., $cl(R_3 + R_4 - 2\infty) = cl(R_4 - R_3)$, $cl(R_5 + R_6 - 2\infty) = cl(R_6 - R_5) \in \operatorname{Ker}\Phi$. In the case: $y_2 = 0$, the same argument implies the same result.

In the later case, since $1 + \frac{2i}{x_1} \neq 0$ or $1 - \frac{2i}{x_1} \neq 0$, (2.2) or (2.3) implies that $y_1 = -y_2$. Therefore we have that $P_2 = \tau(P_1)$, where τ denotes the hyperelliptic involution of C. Hence we have that

$$cl(P_1 + P_2 - 2\infty) = cl(P_1 + \tau(P_1) - 2\infty) = 0. \qquad \blacksquare$$

3. On the Frobenius morphism of a supersingular reduction of *E*

Proposition 3.1. *For any supersingular prime (p) of E, the Legendre symbol $\left(\frac{17}{p}\right)$ is equal to 1.*

Proof. Let

$$\begin{aligned} F_2(x,\, y) = {} & x^3 + y^3 - x^2y^2 + 1488x^2y + 1488xy^2 - 162000x^2 - 162000y^2 \\ & + 40773375xy + 8748000000x + 8748000000y - 157464000000000 \end{aligned}$$

be the modular polynomial of level two. The j-invariant j_E of E is equal to $\frac{2^{14}}{i-4}$. Using Magma we obtain the factorization over $\mathbb{Q}(i)$:

$$\begin{aligned} F_2\left(x,\, \frac{2^{14}}{i-4}\right) = {} & \left\{x + \frac{1}{17^2}(974608 - 292800i)\right\} \\ & \times \left\{x^2 - (19834336 + 8863808i)x - \frac{1}{17}(881201733376 + 313519195136i)\right\}. \end{aligned}$$

Let $f(x)$ be the second factor and D be the discriminant of $f(x)$. By assumption the roots in $\overline{\mathbb{F}}_p$ of the equation $f(x) \equiv 0 \pmod{(p)}$ over $\mathbb{F}_{p^2}$ are supersingular j-invariants, especially they must be contained in $\mathbb{F}_{p^2}$. Therefore we have that $D \bmod (p)$ is a square in $\mathbb{F}_{p^2}$. We obtain the prime decomposition in $\mathbb{Z}[i]$:

$$17D = (1+i)^{24}(2-i)^2(5+2i)^2(7+10i)^2(30+31i)^2(90-61i)^2(1-4i).$$

Multiplying $1+4i$ on both sides and cancelling 17, we have that $1+4i \bmod (p)$ is a square in $\mathbb{F}_{p^2}$. It follows that this is equivalent to $\left(\frac{17}{p}\right) = 1$. (Indeed, $\left(\frac{17}{p}\right) = 1$

implies that a congruence equation $x^2 - x - 4 \equiv 0 \pmod{p}$ has integer solutions a, b. Since $\left(\frac{-1}{p}\right) = -1$, we have $\left(\frac{ab}{p}\right) = -1$. We may assume $\left(\frac{a}{p}\right) = 1$. Therefore there exist integers c, c' such that $c^2 \equiv a \pmod{p}$ and $cc' \equiv 1 \pmod{p}$. Then we have that $(c + 2c'i)^2 \equiv 1 + 4i \pmod{(p)}$.) ■

We consider the field $L(E_1[4])$ generated over $L := \mathbb{Q}(i)$ by the coordinates of all 4-torsion points of E_1.

Lemma 3.2. *$L(E_1[4]) = L(\sqrt{i},\ \sqrt{4-i})$.*

Proof. By replacing x by $x - \frac{4+i}{3}$, we see that E_1 is isomorphic over L to the elliptic curve defined by the equation:

$$y^2 = x^3 + Ax + B, \qquad A = \frac{-15+4i}{3}, \qquad B = \frac{140-50i}{27}.$$

Set $f(x) := x^3 + Ax + B$ and let

$$\psi_4'(x) := x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3$$

be the x-part of the 4th division polynomial (see Exercise 3.7 in [8] (p. 105)). We obtain the prime factorization over L:

$$\begin{aligned}\psi_4'(x) = &\left(x^2 - \frac{8+2i}{3}x + \frac{15-28i}{9}\right)\left(x^2 + \frac{16-2i}{3}x - \frac{81-20i}{9}\right)\\ &\times\left(x^2 - \frac{8-4i}{3}x + \frac{21+20i}{9}\right).\end{aligned}$$

Let α_j and α_j' be the zeros of the jth polynomial in this factorization ($j = 1,\ 2,\ 3$). Then using Magma we obtain that

$$\begin{aligned}L(E_1[4]) &= L(\alpha_j,\ \alpha_j',\ \sqrt{f(\alpha_j)},\ \sqrt{f(\alpha_j')} \mid j = 1,\ 2,\ 3)\\ &= L(\alpha_1,\ \alpha_2) = L(\sqrt{i},\ \sqrt{4-i}).\end{aligned}$$ ■

For an abelian variety B defined over a finite field $\mathbb{F}_q$ and a positive integer r, we denote by $\mathrm{Frob}_{B,\,q^r}$ the q^r-th power Frobenius morphism of B.

Theorem 3.3. *For any supersingular prime (p) of E, it holds that $\mathrm{Frob}_{E_{(p)},\,p^2} = [-p]_{E_{(p)}}$, where $E_{(p)}$ denotes the reduction of E modulo (p) and $[-p]_{E_{(p)}}$ denotes the multiplication by $-p$ map of $E_{(p)}$.*

Proof. Since E and E_1 are isogenous over L, the claim is equivalent to $\mathrm{Frob}_{E_{1(p)},\,p^2} = [-p]_{E_{1(p)}}$. Since $E_{1(p)}$ is supersingular, the multiplication by p map is purely inseparable. Since

$$N_{L/\mathbb{Q}}(j_{E_1}) = \frac{2^8\,241^3}{17^2} \qquad \text{and} \qquad N_{L/\mathbb{Q}}(j_{E_1} - 1728) = 2^8\,5^4\,13^2,$$

we see that $\mathrm{Aut}(E_{1(p)}) = \{\pm 1\}$. Therefore we have that $[p]_{E_{1(p)}} = \pm \mathrm{Frob}_{E_{1(p)},\, p^2}$. The condition $p \equiv 3 \pmod 4$ (resp. Proposition 3.1) implies that $i \bmod (p)$ (resp. $4 - i \bmod (p)$) ($\in \mathbb{F}_{p^2}$) is a square in $\mathbb{F}_{p^2}$. Therefore, by Lemma 3.2, we have that (p) splits completely in $L(E_1[4])$. This implies that $\mathrm{Frob}_{E_{1(p)},\, p^2}$ induces the identity map on $E_{1(p)}[4]$. Hence we have that $\mathrm{Frob}_{E_{1(p)},\, p^2} = [-p]_{E_{1(p)}}$. ∎

For any prime number p which is congruent to 3 modulo 4, we consider the elliptic curve

$$A : y^2 = x^3 - x$$

defined over $\mathbb{F}_p$. Then it is well known that A is supersingular and its endomorphism ring $\mathrm{End}_{\mathbb{F}_{p^2}}(A)$ defined over $\mathbb{F}_{p^2}$ is isomorphic to the maximal order

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\frac{1+\alpha}{2} + \mathbb{Z}\beta + \mathbb{Z}\frac{(1+\alpha)\beta}{2} \qquad (\alpha^2 = -p,\ \beta^2 = -1,\ \beta\alpha = -\alpha\beta)$$

of the quaternion algebra B over $\mathbb{Q}$ ramified precisely at p and ∞ by the correspondence: $\mathrm{Frob}_{A,\, p}$ to α; $I : (x, y) \longmapsto (-x, \sqrt{-1}y)$ to β (see [2]). For any supersingular prime (p) of E, we consider the reduction of Φ (in Theorem 2.1) modulo (p)

$$\Phi_{(p)} : J(C)_p \longrightarrow E_{1(p)} \times E_{1(p)}^{\overline{\sigma}},$$

where $\overline{\sigma}$ denotes the p-th power Frobenius automorphism of $\mathbb{F}_{p^2}$ induced by σ (in Introduction). Let α_p be the group scheme $\mathrm{Spec}\,\overline{\mathbb{F}}_p[X]/(X^p)$ over $\overline{\mathbb{F}}_p$. Since the degree of $\Phi_{(p)}$ is 2^2, we have the dual isogeny

$$\widehat{\Phi_{(p)}} : E_{1(p)} \times E_{1(p)}^{\overline{\sigma}} \longrightarrow J(C)_p$$

with $\widehat{\Phi_{(p)}} \circ \Phi_{(p)} = [4]_{J(C)_p}$ and $\Phi_{(p)} \circ \widehat{\Phi_{(p)}} = [4]_{E_{1(p)} \times E_{1(p)}^{\overline{\sigma}}}$. Then we can consider the two homomorphism of $\overline{\mathbb{F}}_p$-vector spaces:

$$\varphi_1 : \mathrm{Hom}(\alpha_p,\, J(C)_p) \longrightarrow \mathrm{Hom}(\alpha_p,\, E_{1(p)} \times E_{1(p)}^{\overline{\sigma}}), \qquad h \longmapsto \Phi_{(p)} \circ h$$

and

$$\varphi_2 : \mathrm{Hom}(\alpha_p,\, E_{1(p)} \times E_{1(p)}^{\overline{\sigma}}) \longrightarrow \mathrm{Hom}(\alpha_p,\, J(C)_p), \qquad h \longmapsto \widehat{\Phi_{(p)}} \circ h.$$

For any $h \in \mathrm{Hom}(\alpha_p,\, J(C)_p)$, we have $[4]_{J(C)_p} \circ h = h \circ [4]_{\alpha_p}$. Therefore $\varphi_2 \circ \varphi_1$ is the scalar multiplication by 4 map of $\mathrm{Hom}(\alpha_p,\, J(C)_p)$, which is an automorphism of the $\overline{\mathbb{F}}_p$-vector space $\mathrm{Hom}(\alpha_p,\, J(C)_p)$. Similary $\varphi_1 \circ \varphi_2$ is an automorphism of the $\overline{\mathbb{F}}_p$-vector space $\mathrm{Hom}(\alpha_p,\, E_{1(p)} \times E_{1(p)}^{\overline{\sigma}})$. In particular φ_1 is an isomorphism of $\overline{\mathbb{F}}_p$-vector spaces. Hence the dimension of $\mathrm{Hom}(\alpha_p,\, J(C)_p)$ is two. Theorem 2 in [6] implies that there exist two supersingular elliptic curves E_2 and E_3 such that $J(C)_p$ is isomorphic to $E_2 \times E_3$ over $\overline{\mathbb{F}}_p$. On the other hand, by Theorem 3.5 in [7], $E_2 \times E_3$ is isomorphic to $A \times A$ over $\overline{\mathbb{F}}_p$. Hence there exists an isomorphism $\delta : J(C)_p \longrightarrow A \times A$ defined over $\overline{\mathbb{F}}_p$. Since $\mathrm{Frob}_{J(C)_p,\, p^2} = \mathrm{Frob}_{E_{1(p)},\, p^2} \times \mathrm{Frob}_{E_{1(p)}^{\overline{\sigma}},\, p^2} = [-p]_{J(C)_p}$ and $\mathrm{Frob}_{A \times A,\, p^2} = [-p]_{A \times A}$, it holds that $\delta \circ \mathrm{Frob}_{J(C)_p,\, p^2} = \mathrm{Frob}_{A \times A,\, p^2} \circ \delta$, i.e., δ is defined over $\mathbb{F}_{p^2}$.

For any prime p with $\left(\frac{17}{p}\right) = 1$, $x^2+16x-4$ splits completely into linear factors in $\mathbb{F}_p[x]$. Therefore, for any supersingular prime (p) of E, the group $J(C)_p[2](\mathbb{F}_p)$ of $\mathbb{F}_p$-rational 2-torsion points of $J(C)_p$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus 4}$.

Proposition 3.4. *For any supersingular prime* (p) *of* E, $J(C)_p \cong A \times A$ *over* $\mathbb{F}_{p^2}$ *and* $J(C)_p[2](\mathbb{F}_p) \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 4}$.

It is not trivial to answer the question of whether $J(C)_p$ is isomorphic to $A \times A$ over $\mathbb{F}_p$. We next study the surfaces defined over $\mathbb{F}_p$ which are isomorphic to $A \times A$ over $\mathbb{F}_{p^2}$.

4. Restricted quadratic twists of $A \times A$

Set

$$\mathrm{Twist}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A) := \left\{ [B] \;\middle|\; \begin{array}{l} B \text{ is an abelian surface defined over } \mathbb{F}_p \\ \text{such that } B \cong A \times A \text{ over } \mathbb{F}_{p^2} \end{array} \right\},$$

where $[B]$ denotes the isomorphism class over $\mathbb{F}_p$ represented by B and

$$\mathrm{Twist}^{(4)}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A) := \{[B] \in \mathrm{Twist}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A) \mid B[2](\mathbb{F}_p) \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 4}\}.$$

In this section we construct all the elements of $\mathrm{Twist}^{(4)}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A)$ explicitly by following the paper of C. F. Yu [11]. In the following we restrict the arguments in [11] to the case where the dimension is two.

Yu considers the set

$$\mathcal{S} := \left\{ [B] \;\middle|\; \begin{array}{l} B \text{ is an abelian surface defined over } \mathbb{F}_p \\ \text{such that } B \text{ is isogenous to } A \times A \text{ over } \mathbb{F}_p \end{array} \right\}.$$

Then we have that

$$\mathcal{S} = \mathrm{Twist}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A).$$

Indeed, for any $[B] \in \mathcal{S}$, Lemma 2.2 in [11] implies that B is superspecial (i.e., isomorphic to a product of two supersingular elliptic curves). By Theorem 3.5 in [7], we get that B is isomorphic to $A \times A$ over $\overline{\mathbb{F}}_p$. Lemma 2.2 in [11] also implies that $\mathrm{Frob}_{B,\,p^2} = \mathrm{Frob}^2_{B,\,p} = -p$. By the above arguments in Section 3, we obtain that B is isomorphic to $A \times A$ over $\mathbb{F}_{p^2}$. So we have $[B] \in \mathrm{Twist}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A)$. Conversely, for any $[B] \in \mathrm{Twist}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A)$, we have that $\mathrm{Frob}^2_{B,\,p} = \mathrm{Frob}_{B,\,p^2} = \mathrm{Frob}_{A,\,p^2} \times \mathrm{Frob}_{A,\,p^2} = [-p]_B$. So the characteristic polynomial of $\mathrm{Frob}_{B,\,p}$ is $(X^2 + p)^2$, which coincides with that of $\mathrm{Frob}_{A \times A,\,p}$. A theorem of Tate (Theorem 1 (c) in [10]) implies that B is isogenous to $A \times A$ over $\mathbb{F}_p$.

We will take $A \times A$ as a fixed abelian variety A_0 in Section 3 of [11]. Let $\mathcal{R}$ and $\mathcal{K}$ denote $\mathbb{Z}[\sqrt{-p}]$ and $\mathbb{Q}(\sqrt{-p})$, respectively. Set $\overline{\mathcal{R}} := \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$. Let $T_\ell(A \times A)$ be the ℓ-adic Tate module of $A \times A$ for any prime $\ell \neq p$ and let

$M(A \times A)$ be the covariant Dieudonné module of $A \times A$. Since the endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(A \times A)$ of $A \times A$ defined over $\mathbb{F}_p$ is isomorphic to $M_2(\overline{\mathcal{R}})$, $T_\ell(A \times A)$ (resp. $M(A \times A)$) has the structure of $\overline{\mathcal{R}} \otimes \mathbb{Z}_\ell$ (resp. $\overline{\mathcal{R}} \otimes \mathbb{Z}_p$)-modules compatible with $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-action. For any prime ℓ', $\overline{\mathcal{R}} \otimes \mathbb{Z}_{\ell'}$ is a DVR or a product of DVRs. Therefore $T_\ell(A \times A)$ (resp. $M(A \times A)$) is a free $\overline{\mathcal{R}} \otimes \mathbb{Z}_\ell$ (resp. $\overline{\mathcal{R}} \otimes \mathbb{Z}_p$)-module of rank 2, i.e., we have that

$$T_\ell(A \times A) \cong (\overline{\mathcal{R}} \oplus \overline{\mathcal{R}}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$$

for any prime $\ell \neq p$ and

$$M(A \times A) \cong (\overline{\mathcal{R}} \oplus \overline{\mathcal{R}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Therefore on the isomorphism $(*)$

$$T(A \times A) \otimes_{\widehat{\mathbb{Z}}} \mathbb{A}_f \cong (\mathcal{K} \oplus \mathcal{K}) \otimes_{\mathbb{Q}} \mathbb{A}_f$$

in the proof of Theorem 3.1 in [11], where

$$T(A \times A) = M(A \times A) \times \prod_{\ell \neq p} T_\ell(A \times A),$$

we can assume that

$$\overline{\mathcal{R}} \oplus \overline{\mathcal{R}} = \{v \in \mathcal{K} \oplus \mathcal{K} \mid v \otimes 1 \in T(A \times A)\}.$$

For any $[B] \in \mathrm{Twist}^{(4)}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A) \subseteq \mathcal{S}$, we have an isogeny $f : B \longrightarrow A \times A$ defined over $\mathbb{F}_p$. On the other hand, since $B[2]$ is contained in $\mathrm{Ker}(1 + \mathrm{Frob}_{B,\,p})$, we have that $\frac{1+\mathrm{Frob}_{B,\,p}}{2}$ is an element of $\mathrm{End}_{\mathbb{F}_p}(B)$, i.e., $\overline{\mathcal{R}} \subseteq \mathrm{End}_{\mathbb{F}_p}(B)$. So the lattice corresponding to B

$$\{v \in \overline{\mathcal{R}} \oplus \overline{\mathcal{R}} \mid v \otimes 1 \in f_*(T(B))\}$$

has the structure of $\overline{\mathcal{R}}$-module. Thus we obtain that on the correspondence of Theorem 3.1 in [11], elements of $\mathrm{Twist}^{(4)}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A)$ correspond to isomorphism classes of finitely generated $\overline{\mathcal{R}}$-submodules of $\overline{\mathcal{R}} \oplus \overline{\mathcal{R}}$ of rank two.

For any ideal $\mathfrak{a}$ in $\overline{\mathcal{R}} \cong \mathrm{End}_{\mathbb{F}_p}(A)$, we set $A[\mathfrak{a}] := \{P \in A \mid a(P) = O \text{ for } \forall a \in \mathfrak{a}\}$ and $A_{\mathfrak{a}} := A/A[\mathfrak{a}]$. Since $A[\mathfrak{a}]$ is invariant under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, $A_{\mathfrak{a}}$ is defined over $\mathbb{F}_p$. Let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_h\}$ be a complete set of representatives of the ideal class group of $\mathcal{K}$ such that $\mathfrak{q}_j$ $(1 \leqslant j \leqslant h)$ is a prime ideal lying over an odd prime number q_j which splits in $\mathcal{K}$. Then $\{\overline{\mathfrak{q}}_1, \ldots, \overline{\mathfrak{q}}_h\}$ is also a complete set of representatives, where $\overline{\mathfrak{q}}_j := \{\overline{v} \mid v \in \mathfrak{q}_j\}$ and $\overline{v}$ denotes the image of v by the automorphism of $\overline{\mathcal{R}}$ sending $\frac{1+\sqrt{-p}}{2}$ to $\frac{1-\sqrt{-p}}{2}$. It is well known from the general theory of modules over Dedekind domains that $\{\overline{\mathcal{R}} \oplus \overline{\mathfrak{q}}_1, \ldots, \overline{\mathcal{R}} \oplus \overline{\mathfrak{q}}_h\}$ becomes a complete set of representatives of the set of isomorphism classes of finitely generated torsion-free $\overline{\mathcal{R}}$-modules of rank two. For $1 \leqslant j \leqslant h$, we set

$$\pi_j : A \times A_{\mathfrak{q}_j} \longrightarrow A \times A, \qquad (P, \overline{Q}) \longmapsto (P, q_j Q) \ \ (P, Q \in A).$$

Then it is easily seen that

$$\overline{\mathcal{R}} \oplus \overline{\mathfrak{q}}_j = \{v \in \overline{\mathcal{R}} \oplus \overline{\mathcal{R}} \,|\, v \otimes 1 \in \pi_{j*}(A \times A_{\mathfrak{q}_j})\}$$

$(1 \leqslant j \leqslant h)$. Consequently, we have obtained the following:

Theorem 4.1. $\mathrm{Twist}^{(4)}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A \times A) = \{[A \times A_{\mathfrak{q}_1}], \ldots, [A \times A_{\mathfrak{q}_h}]\}$.

5. A property of $J(C)_p$ over $\mathbb{F}_p$

In this section we prove that for any supersingular prime (p) of E, $J(C)_p$ is isomorphic to $A \times A$ over $\mathbb{F}_p$. More generally, we show the following:

Theorem 5.1. *Let p be a prime number such that (i) $p \equiv 3 \pmod 4$; (ii) $p \neq 3$ and $\mathfrak{q}$ be an element of $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_h\}$. Let $\overline{\sigma}$ be the p-th power Frobenius automorphism of $\overline{\mathbb{F}}_p$. Assume that there exist an irreducible principal polarization D on $A \times A_{\mathfrak{q}}$ and an automorphism ε of $A \times A_{\mathfrak{q}}$ with $\varepsilon^2 = 1$ such that*

(i) *$D^{\overline{\sigma}}$ is algebraically equivalent to D (this is denoted by $D^{\overline{\sigma}} \equiv D$);*
(ii) *$\varepsilon^* D \equiv D$;*
(iii) *$\varepsilon^{\overline{\sigma}} = -\varepsilon$.*

Then we have that $\mathfrak{q}$ is principal, i.e., $A \times A_{\mathfrak{q}} \cong A \times A$ over $\mathbb{F}_p$.

We note that for any supersingular prime (p) of E, the principally polarized abelian surface $(J(C)_p, \Theta)$ ($\Theta := \{cl(P - \infty) \,|\, P \in C_p\}$) satisfies the assumptions in Theorem 5.1. In fact, Proposition 3.4 and Theorem 4.1 imply that $J(C)_p \cong A \times A_{\mathfrak{q}}$ over $\mathbb{F}_p$ for some $\mathfrak{q}$. Let

$$\overline{\eta} : J(C)_p \longrightarrow J(C)_p,$$

$$cl(P_1 + P_2 - 2\infty) \longmapsto cl(\eta(P_1) + \eta(P_2) - 2\eta(\infty)) = cl(\eta(P_1) + \eta(P_2) - 2\infty),$$

where η is the automorphism of C defined in Section 2 ($\eta(\infty) = (0, 0) = R_2$). Then it follows that $\overline{\eta}(0) = 0$ and $\overline{\eta}^2 = 1$, i.e., $\overline{\eta}$ is an automorphism of $A \times A_{\mathfrak{q}}$ with order 2. We can easily check that $\Theta^{\overline{\sigma}} = \Theta$, $\overline{\eta}^* \Theta = \Theta + cl(\infty - R_2) \equiv \Theta$ and $\overline{\eta}^{\overline{\sigma}} = -\overline{\eta}$.

The strategy for proving Theorem 5.1 is that we derive the following simultaneous equations (5.6) from the assumptions in Theorem 5.1 and solve (5.6) by using a Groebner basis and construct a generator of $\mathfrak{q}$ from some integral solution of (5.6).

By the identification

$$\mathrm{End}_{\mathbb{F}_{p^2}}(A) \cong \mathcal{O} \cong \overline{\mathcal{R}} \oplus \overline{\mathcal{R}}\beta$$

(the first is explained in Section 3 and the second is done by assigning α to $\sqrt{-p}$), it is obtained that

$$\begin{aligned}\mathrm{End}_{\overline{\mathbb{F}}_p}(A\times A_{\mathfrak{q}}) &= \mathrm{End}_{\mathbb{F}_{p^2}}(A\times A_{\mathfrak{q}})\\ &\cong \left\{\begin{pmatrix}\gamma_1 & \gamma_2\\ \gamma_3 & \gamma_4\end{pmatrix}\ \middle|\ \begin{array}{ll}\gamma_1\in\overline{\mathcal{R}}+\overline{\mathcal{R}}\beta, & \gamma_2\in\mathfrak{q}+\overline{\mathfrak{q}}\beta\\ \gamma_3\in\mathfrak{q}^{-1}+\mathfrak{q}^{-1}\beta, & \gamma_4\in\overline{\mathcal{R}}+\mathfrak{q}^{-1}\overline{\mathfrak{q}}\beta\end{array}\right\}\\ &=: \begin{pmatrix}\overline{\mathcal{R}}+\overline{\mathcal{R}}\beta & \mathfrak{q}+\overline{\mathfrak{q}}\beta\\ \mathfrak{q}^{-1}+\mathfrak{q}^{-1}\beta & \overline{\mathcal{R}}+\mathfrak{q}^{-1}\overline{\mathfrak{q}}\beta\end{pmatrix}.\end{aligned}$$

Through this identification, the action of $\overline{\sigma}$ on $M_2(\mathcal{K})+M_2(\mathcal{K})\beta$ ($\cong \mathrm{End}_{\mathbb{F}_{p^2}}(A\times A_{\mathfrak{q}})\otimes_{\mathbb{Z}}\mathbb{Q}$) is given by

$$(U+V\beta)^{\overline{\sigma}} = U - V\beta$$

for any $U,\ V\in M_2(\mathcal{K})$. We set $X := A\times\{\overline{O}\}+\{O\}\times A_{\mathfrak{q}}$ and consider

$$\phi_X : A\times A_{\mathfrak{q}} \xrightarrow{\sim} \mathrm{Pic}^0(A\times A_{\mathfrak{q}}),\qquad (P,\overline{Q})\longmapsto cl(T^*_{(P,\overline{Q})}X - X),$$

where $T^*_{(P,\overline{Q})}X$ denotes the pullback of the divisor X by the morphism $T_{(P,\overline{Q})}$: $A\times A_{\mathfrak{q}}\to A\times A_{\mathfrak{q}},\ \ Z\mapsto Z+(P,\overline{Q})$. It is easy to check that the Rosati involution ι on $\mathrm{End}_{\mathbb{F}_{p^2}}(A\times A_{\mathfrak{q}})\otimes_{\mathbb{Z}}\mathbb{Q}$ with respect to X is given by

$$\iota : M_2(B)\ni\begin{pmatrix}\gamma_1 & \gamma_2\\ \gamma_3 & \gamma_4\end{pmatrix}\longmapsto\begin{pmatrix}\overline{\gamma_1} & q\overline{\gamma_3}\\ \frac{\overline{\gamma_2}}{q} & \overline{\gamma_4}\end{pmatrix}\in M_2(B),$$

where for $\gamma = u_1+u_2\beta$ $(u_1,\ u_2\in\mathcal{K})$, $\overline{\gamma}$ denotes $\overline{u_1}-u_2\beta$, the image of γ under the main involution of the quaternion algebra B in Section 3 and q is the prime number lying under $\mathfrak{q}$.

Since $\phi_X^{-1}\circ\phi_D$ is contained in $\mathrm{Aut}_{\overline{\mathbb{F}}_p}(A\times A_{\mathfrak{q}})\cong\begin{pmatrix}\overline{\mathcal{R}} & \mathfrak{q}\\ \mathfrak{q}^{-1} & \overline{\mathcal{R}}\end{pmatrix}^{\times}$ and fixed by the Rosati involution with respect to X (see p. 190 in [4]), there exist $r\in\overline{\mathfrak{q}}$ and $s,\ t\in\mathbb{Z}$ such that

$$\phi_X^{-1}\circ\phi_D = \begin{pmatrix}s & \overline{r}\\ \frac{r}{q} & t\end{pmatrix}.$$

Since $\phi_X^{-1}\circ\phi_D$ is positive definite (see Prop. 2.8 in [3]) and $\overline{\mathcal{R}}^{\times}=\{\pm1\}$, it holds that $s>0$, $t>0$ and

$$st-\frac{r\overline{r}}{q}=1. \tag{5.1}$$

By assumption ε is expressed in the form:

$$\varepsilon = \begin{pmatrix}x & y\\ z & w\end{pmatrix}\beta\qquad (x\in\overline{\mathcal{R}},\ \ y\in\overline{\mathfrak{q}},\ \ z\in\mathfrak{q}^{-1}=\frac{1}{q}\overline{\mathfrak{q}},\ \ w\in\mathfrak{q}^{-1}\overline{\mathfrak{q}}=\frac{1}{q}\overline{\mathfrak{q}}^2).$$

Since $\varepsilon^2 = 1$, we obtain four equations:

$$\left.\begin{aligned} x\overline{x} + y\overline{z} &= -1,\\ w\overline{w} + z\overline{y} &= -1,\\ x\overline{y} + y\overline{w} &= 0,\\ z\overline{x} + w\overline{z} &= 0. \end{aligned}\right\} \tag{5.2}$$

By assumption we obtain that $\phi_{\varepsilon^* D} = \phi_D$, hence $\widehat{\varepsilon} \circ \phi_D \circ \varepsilon = \phi_D$, where $\widehat{\varepsilon}$ denotes the induced map $\mathrm{Pic}^0(A \times A_{\mathfrak{q}}) \to \mathrm{Pic}^0(A \times A_{\mathfrak{q}})$ from ε by the pullback of line bundles. Therefore we have that

$$\widehat{\varepsilon} \circ \phi_X \circ \begin{pmatrix} s & \overline{r} \\ \frac{r}{q} & t \end{pmatrix} \circ \varepsilon = \phi_X \circ \begin{pmatrix} s & \overline{r} \\ \frac{r}{q} & t \end{pmatrix}.$$

Since

$$\phi_X^{-1} \circ \widehat{\varepsilon} \circ \phi_X = \iota(\varepsilon) = -\begin{pmatrix} x & qz \\ \frac{y}{q} & w \end{pmatrix} \beta,$$

we obtain three equations:

$$\left.\begin{aligned} sx + \overline{r}z &= 0,\\ \tfrac{ry}{q} + tw &= 0,\\ rx + qtz &= -sy - \overline{r}w. \end{aligned}\right\} \tag{5.3}$$

We also have that

$$\phi_X^{-1} \circ \phi_{\varepsilon^* X} = \phi_X^{-1} \circ \widehat{\varepsilon} \circ \phi_X \circ \varepsilon = \iota(\varepsilon) \circ \varepsilon = \begin{pmatrix} x\overline{x} + qz\overline{z} & x\overline{y} + qz\overline{w} \\ \frac{y\overline{x}}{q} + w\overline{z} & \frac{y\overline{y}}{q} + w\overline{w} \end{pmatrix}.$$

Since $\varepsilon^* X$ is principal, its determinant is equal to 1. Therefore we obtain one equation

$$(x\overline{x} + qz\overline{z})(y\overline{y} + qw\overline{w}) - (x\overline{y} + qz\overline{w})(y\overline{x} + qw\overline{z}) = q. \tag{5.4}$$

To solve the simultaneous equations (5.1), (5.2), (5.3) and (5.4), we introduce the canonical basis of $\overline{\mathcal{R}}$, $\overline{\mathfrak{q}}$ and $\overline{\mathfrak{q}}^2$. We put $\omega := \frac{1+\sqrt{-p}}{2}$. Then $\overline{\mathcal{R}} = [1,\, \omega]$. It is well known that we can take $a,\ b \in \mathbb{Z}$ such that

$$\left.\begin{aligned} &\text{(i)}\ \ 0 \leqslant a \leqslant q-1,\ 0 \leqslant b \leqslant q^2 - 1;\\ &\text{(ii)}\ \ a^2 + a + \tfrac{p+1}{4} = kq,\quad b^2 + b + \tfrac{p+1}{4} = \ell q^2 \ \text{(for some } k,\ \ell \in \mathbb{N});\\ &\text{(iii)}\ \ b - a = mq \ \text{(for some } m \in \mathbb{Z});\\ &\text{(iv)}\ \ \overline{\mathfrak{q}} = [q,\, a+\omega],\ \overline{\mathfrak{q}}^2 = [q^2,\, b+\omega]. \end{aligned}\right\} \tag{5.5}$$

(For any non-zero ideal $\mathfrak{a}$ of $\overline{\mathcal{R}}$, let a_0 be the minimum positive integer in $\mathfrak{a}$ and let $b_0 + c_0\omega$ be an element of $\mathfrak{a}$ such that the coefficient of ω is minimum positive. Then it follows that $\mathfrak{a} = [a_0,\, b_0 + c_0\omega]$ and both a_0 and b_0 are divisible by c_0. Therefore we have that $\mathfrak{a} = c_0[a_1,\, b_1 + \omega]$, where $a_0 = c_0 a_1$ and $b_0 = c_0 b_1$. Since $\overline{\mathfrak{q}}$ splits in $\mathbb{Q}(\sqrt{-p})$, we have $c_0 = 1$ for $\overline{\mathfrak{q}}$ and $\overline{\mathfrak{q}}^2$.)

By reselecting $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_h\}$ if necessary, we can assume that $q_j > \frac{p+1}{4}$ for $1 \leqslant j \leqslant h$. Therefore we can add the conditions that $a \neq 0$ and $b \neq 0$. We set

$$r = qr_1 + r_2(a+\omega), \quad x = x_1 + x_2\omega, \quad y = qy_1 + y_2(a+\omega),$$
$$z = z_1 + z_2\frac{a+\omega}{q}, \quad w = qw_1 + w_2\frac{b+\omega}{q}$$

($r_1,\ r_2,\ x_1,\ x_2,\ y_1,\ y_2,\ z_1,\ z_2,\ w_1,\ w_2 \in \mathbb{Z}$). Using $\omega^2 - \omega + \frac{p+1}{4} = 0$ and the relations (ii) and (iii) in (5.5), we get the following simultaneous equations with respect to s, t, r_1, r_2, x_1, x_2, y_1, y_2, z_1, z_2, w_1, w_2 from (5.1), (5.2), (5.3) and (5.4) by comparing coefficients of 1 and ω:

$$\left.\begin{array}{l}
\bullet\ qr_1^2 + (2a+1)r_1r_2 + kr_2^2 - st + 1 = 0,\\
\bullet\ x_1^2 + x_1x_2 + \frac{p+1}{4}x_2^2 + qy_1z_1 + (2a+1)y_1z_2 + ky_2z_2 + 1 = 0,\\
\bullet\ y_1z_2 - y_2z_1 = 0,\\
\bullet\ q^2w_1^2 + (2b+1)w_1w_2 + \ell w_2^2 + qy_1z_1 + (2a+1)y_1z_2 + ky_2z_2 + 1 = 0,\\
\bullet\ qx_1y_1 + x_1y_2 + \frac{p+1}{4}x_2y_2 + q^2y_1w_1 + y_1w_2 + aqy_2w_1 + (k+am)y_2w_2 = 0,\\
\bullet\ x_1y_2 - qx_2y_1 - ax_2y_2 + y_1w_2 - qy_2w_1 - my_2w_2 = 0,\\
\bullet\ x_1z_1 + x_2z_1 + \frac{a}{q}x_1z_2 + \frac{1}{q}(a + \frac{p+1}{4})x_2z_2 + qz_1w_1 + (a+1)z_2w_1 + \frac{b}{q}z_1w_2\\
\quad +(\ell - \frac{bm}{q})z_2w_2 = 0,\\
\bullet\ x_2z_1 - \frac{1}{q}x_1z_2 + \frac{a}{q}x_2z_2 + z_2w_1 - \frac{1}{q}z_1w_2 + \frac{m}{q}z_2w_2 = 0,\\
\bullet\ sx_2 + r_1z_2 - r_2z_1 = 0,\\
\bullet\ sx_1 + qr_1z_1 + ar_1z_2 + (a+1)r_2z_1 + kr_2z_2 = 0,\\
\bullet\ qr_1y_1 + ar_1y_2 + ar_2y_1 + (k - \frac{a}{q} - \frac{1}{q}\cdot\frac{p+1}{2})r_2y_2 + qtw_1 + \frac{b}{q}tw_2 = 0,\\
\bullet\ r_1y_2 + r_2y_1 + \frac{1}{q}(2a+1)r_2y_2 + \frac{1}{q}tw_2 = 0,\\
\bullet\ qr_1x_1 + ar_2x_1 - \frac{p+1}{4}r_2x_2 + qtz_1 + atz_2 + qsy_1 + asy_2 + q^2r_1w_1 + br_1w_2\\
\quad +q(a+1)r_2w_1 + (q\ell - bm)r_2w_2 = 0,\\
\bullet\ qr_1x_2 + r_2x_1 + (a+1)r_2x_2 + tz_2 + sy_2 + r_1w_2 - qr_2w_1 - mr_2w_2 = 0,\\
\bullet\ (x_1^2 + x_1x_2 + \frac{p+1}{4}x_2^2 + qz_1^2 + (2a+1)z_1z_2 + kz_2^2)\\
\quad \times(q^2y_1^2 + q(2a+1)y_1y_2 + qky_2^2 + q^3w_1^2 + q(2b+1)w_1w_2 + q\ell w_2^2)\\
\quad -(q^2w_1^2 + (2b+1)w_1w_2 + \ell w_2^2)(q^2z_1^2 + q(2a+1)z_1z_2 + qkz_2^2 - 2q^2y_1z_1\\
\quad -q(4a+2)y_1z_2 - 2qky_2z_2 + q^2y_1^2 + q(2a+1)y_1y_2 + qky_2^2) - q = 0.
\end{array}\right\} \tag{5.6}$$

We compute a Groebner basis of the ideal associated to (5.6) by using Magma V2.19-7. For this we view m, ℓ, k, b, a, q, p as indeterminates and consider the residue class ring

$$R := \mathbb{Q}[m,\ k,\ \ell,\ p,\ q,\ a,\ b]/(a^2 + a + \frac{p+1}{4} - qk,\ b^2 + b + \frac{p+1}{4} - q^2\ell,$$
$$b - a - qm,\ m(a+b+1) - q\ell + k)$$

because of that the relations (ii) and (iii) in (5.5) imply $q(m(a+b+1) - q\ell + k) = 0$.

Then we can see that the simultaneous equations

$$\begin{cases} \bullet\ a^2 + a + \frac{p+1}{4} - qk = 0, \\ \bullet\ b^2 + b + \frac{p+1}{4} - q^2\ell = 0, \\ \bullet\ b - a - qm = 0, \\ \bullet\ m(a+b+1) - q\ell + k = 0 \end{cases}$$

is equivalent to

$$\begin{cases} \bullet\ b = a + qm, \\ \bullet\ k = q\ell - qm^2 - (2a+1)m, \\ \bullet\ p = 4q^2\ell - 4a^2 - 4a - 4q^2m^2 - 4(2a+1)qm - 1. \end{cases}$$

So R is isomorphic to a polynomial ring in four variable over $\mathbb{Q}$. Therefore we can consider the field of fractions of R, denoted by K. Let $f_1, \ldots, f_{15}$ be the polynomials appearing in the left hand sides of equations in (5.6) in turn. Put

$$J := (f_1, \ldots, f_{15}),$$

the ideal in the polynomial ring $K[s,\ t,\ r_1,\ r_2,\ x_1,\ x_2,\ y_1,\ y_2,\ z_1,\ z_2,\ w_1,\ w_2]$. In this setting, we can compute a Groebner basis of J by Magma. It should be remarked that the Groebner basis is computed using the standard lexicographical order of variables (default in Magma). We denote the resulting basis by G (see [5] for Magma's commands to calculate G and $I_1, \ldots, I_8$ defined in the following paragraphs). Then the number of the elements of G is 48. The 48th element of G, denoted by $G[48]$, is a polynomial with respect to z_1, z_2, w_1 and w_2 only and has the factorization:

$$\begin{aligned} &(w_1^2 + \frac{2b+1}{q^2} w_1 w_2 + \frac{4b^2+4b+p+1}{4q^4} w_2^2 + \frac{1}{q^2}) \\ &\quad \times (z_1^3 w_2 - \frac{aq}{b} z_1^2 z_2 w_1 + \frac{ab-a+b}{qb} z_1^2 z_2 w_2 - \frac{2a^2}{b} z_1 z_2^2 w_1 \\ &\quad + \frac{-4a^2b - 2pa - 8a^2 + pb + 4ab - 2a + b}{4q^2b} z_1 z_2^2 w_2 + \frac{-4a^3 + pa + a}{4qb} z_2^3 w_1 \\ &\quad + \frac{-4a^3b - 2pa^2 - 4a^3 + pab - 2a^2 + ab}{4q^3b} z_2^3 w_2). \end{aligned}$$

The assumptions in Theorem 5.1 imply an integral solution of the simultaneous equations associated to G. From now on $(s, t, r_1, r_2, x_1, x_2, y_1, y_2, z_1, z_2, w_1, w_2)$ denotes one integral solution of the simultaneous equations associated to G, not indeterminates.

The first factor in this factorization is equal to

$$(w_1 + \frac{2b+1}{2q^2} w_2)^2 + \frac{p}{4q^4} w_2^2 + \frac{1}{q^2}.$$

Since the first two summands are non-negative and the last is positive, we have that the first factor is a positive rational number. Therefore the second factor is zero. The second factor is equal to

$$\begin{aligned}&-\frac{a}{qb}z_2(q^2z_1^2+2aqz_1z_2+\frac{4a^2-p-1}{4}z_2^2)w_1\\&+w_2(z_1+\frac{a}{q}z_2)(z_1^2+\frac{-a+b}{qb}z_1z_2+\frac{-4a^2b-2pa-4a^2+pb-2a+b}{4q^2b}z_2^2). \quad (5.7)\end{aligned}$$

Lemma 5.2. $z_2(q^2z_1^2+2aqz_1z_2+\frac{4a^2-p-1}{4}z_2^2)\neq 0$.

Proof. We suppose that $z_2=0$. Then (5.7) implies $w_2z_1^3=0$. If $z_1=0$, then $z=0$ and this contradicts the first equation in (5.2). If $w_2=0$, then the 4th equation in (5.6) implies that $q^2w_1^2+qy_1z_1+1=0$. Hence we have that $1\equiv 0 \pmod q$, a contradiction. Therefore $z_2\neq 0$.

The discriminant of the quadratic polynomial $q^2T^2+2aqT+\frac{4a^2-p-1}{4}$ is $q^2(p+1)$. This is not a square because of $p\neq 3$. Hence the equation $q^2T^2+2aqT+\frac{4a^2-p-1}{4}=0$ has no rational roots. ■

We obtain the fractional expression of w_1 with respect to z_1, z_2 and w_2, denoted by I_1 (therefore $w_1=I_1$).

$G[47]$ is a polynomial with respect to y_2, z_1, z_2, w_1 and w_2 and the degree of $G[47]$ with respect to y_2 is 1. The coefficient of y_2 in $G[47]$ is

$$z_2^3(w_1^2+\frac{2b+1}{q^2}w_1w_2+\frac{4b^2+p+4b+1}{4q^4}w_2^2).$$

Lemma 5.3. $w_1^2+\frac{2b+1}{q^2}w_1w_2+\frac{4b^2+p+4b+1}{4q^4}w_2^2\neq 0$.

Proof. We suppose that $w_2=0$. By (5.7) and Lemma 5.2, we have $w_1=0$, i.e., $w=0$. By the second equation in (5.3), we have that $y=0$ or $r=0$. If $r=0$, then $D\equiv X$. This contradicts the assumption that D is irreducible. Therefore $y=0$. This contradicts the first equation in (5.2). Therefore $w_2\neq 0$.

The discriminant of the quadratic polynomial $T^2+\frac{2b+1}{q^2}T+\frac{4b^2+p+4b+1}{4q^4}$ is $-\frac{p}{q^4}$. Hence the equation $T^2+\frac{2b+1}{q^2}T+\frac{4b^2+p+4b+1}{4q^4}=0$ has no real roots. ■

We obtain the fractional expression of y_2 with respect to z_1, z_2, w_1 and w_2. By substituting I_1 for w_1, we obtain the fractional expression of y_2 with respect to z_1, z_2 and w_2, denoted by I_2.

We see that y_1 does not appear in $G[n]$ $(n=46,\ldots,42)$.

The degree of $G[41]$ with respect to y_1 is 1 and the coefficient of y_1 is

$$w_2(w_1^2+\frac{2b+1}{q^2}w_1w_2+\frac{4b^2+p+4b+1}{4q^4}w_2^2+\frac{1}{q^2}).$$

By the same arguments as above, we see that it is non-zero. Therefore we obtain the fractional expression of y_1 with respect to z_1, z_2 and w_2, denoted by I_3.

Next we obtain the fractional expression I_4 (resp. I_5) of x_2 (resp. x_1) with respect to z_1, z_2 and w_2 from $G[37]$ (resp. $G[30]$).

The polynomial $G[24]$ is equal to

$$r_2^2 - \frac{2q^2}{p}x_1w_1 - \frac{2b+1}{p}x_1w_2 - \frac{q^2}{p}x_2w_1 - \frac{p+2b+1}{2p}x_2w_2 - \frac{2q^3}{p}w_1^2 - \frac{4qb+2q}{p}w_1w_2 - \frac{4b^2+p+4b+1}{2pq}w_2^2.$$

By substituting I_1, I_4 and I_5 and setting $u := \pm\sqrt{qz_1^2+(2a+1)z_1z_2+kz_2^2}$, we obtain

$$r_2 = \frac{m}{a} \cdot \frac{w_2(z_1 + \frac{a^2}{qa-qb}z_2)}{z_1^2 + \frac{2a}{q}z_1z_2 + \frac{4a^2-p-1}{4q^2}z_2^2} \cdot u \ (=: I_6u).$$

The degree of $G[23]$, $G[22]$ and $G[21]$ with respect to r_1 are all 1. But $G[21]$ is fairly shorter than $G[23]$ and $G[22]$. The coefficient of r_1 in $G[21]$ is equal to

$$z_1w_2 - qz_2w_1 + \frac{a-b}{q}z_2w_2. \tag{5.8}$$

Lemma 5.4. $z_1w_2 - qz_2w_1 + \frac{a-b}{q}z_2w_2 \neq 0$.

Proof. We assume that $z_1w_2 - qz_2w_1 + \frac{a-b}{q}z_2w_2 = 0$. Then the resultant of (5.7) and (5.8) with respect to w_1 is 0. On the other hand this resultant is equal to

$$\frac{q(b-a)}{b}w_2z_2\left(z_1 + \frac{a^2}{q(a-b)}z_2\right)\left(z_1^2 + \frac{2a+1}{q}z_1z_2 + \frac{4a^2+p+4a+1}{4q^2}z_2^2\right).$$

Therefore we have that $z_1 + \frac{a^2}{q(a-b)}z_2 = 0$. By substituting $\frac{a^2}{q(b-a)}z_2$ for z_1 in the assumption and dividing by z_2, we also have that $w_1 + \frac{2ab-b^2}{q^2(a-b)}w_2 = 0$. By substituting $\frac{a^2}{q(b-a)}z_2$ and $\frac{2ab-b^2}{q^2(b-a)}w_2$ for z_1 and w_1, respectively, in $G[47]$ and factoring it, we have that

$$y_2z_2 + \frac{1}{q}w_2^2 + \frac{4q^3m^2}{4a^2b^2+qm(pqm+4ab+qm)} = 0.$$

In particular $\frac{4q^4m^2}{4a^2b^2+qm(pqm+4ab+qm)}$ is an integer. Since q and $4ab$ are coprime, $4a^2b^2+qm(pqm+4ab+qm)$ divides $4m^2$. Especially

$$4m^2 \geqslant 4a^2b^2 + qm(pqm+4ab+qm) > q^2m^2 > 4m^2.$$

This is a contradiction. ∎

Therefore we obtain that

$$r_1 = I_7 u$$

for some fractional expression I_7 with respect to z_1, z_2 and w_2.

The polynomial $G[8]$ is

$$tw_2 + qr_1y_2 + qr_2y_1 + (2a+1)r_2y_2.$$

It is proved that $w_2 \neq 0$ in the proof of Lemma 5.3. Therefor we get $t = I_8 u$ for some fractional expression I_8 with respect to z_1, z_2 and w_2.

Finally, from $G[1]$, we obtain that

$$s = -u.$$

Lemma 5.5. *Let T, Z_1, Z_2, W_2 be indeterminates and we regard $I_n = I_n(Z_1, Z_2, W_2)$ as the fractional expressions with respect to Z_1, Z_2 and W_2 $(1 \leqslant n \leqslant 8)$. Then we have that*

(1) $I_n(TZ_1, TZ_2, W_2) = I_n(Z_1, Z_2, W_2)$ *for* $n = 1,\ 4,\ 5$;
(2) $I_n(TZ_1, TZ_2, W_2) = \frac{1}{T} I_n(Z_1, Z_2, W_2)$ *for* $n = 2,\ 3,\ 6,\ 7$;
(3) $I_8(TZ_1, TZ_2, W_2) = \frac{1}{T^2} I_8(Z_1, Z_2, W_2)$.

Proof. They are checked by Magma. See [5]. ∎

Let d be the greatest common divisor of z_1 and z_2 and set $z_n = z'_n d$ $(n = 1,\ 2)$. By Lemma 5.5,

$$\left(\frac{s}{d},\ dt,\ r_1,\ r_2,\ x_1,\ x_2,\ dy_1,\ dy_2,\ z'_1,\ z'_2,\ w_1,\ w_2\right)$$

is also a solution. But d^2 divides $qz_1^2 + (2a+1)z_1z_2 + kz_2^2 = u^2 = s^2$. Hence it is an integral solution. Therefore we may assume that z_1 and z_2 are coprime.

Lemma 5.6. *We have the following relations:*

(1) $x_2 = z_2\frac{r_1}{u} - z_1\frac{r_2}{u}$;
(2) $w_2 = -qz_2\frac{r_1}{u} - (qz_1 + (2a+1)z_2)\frac{r_2}{u}$.

Proof. Using the fractional expressions $\frac{r_1}{u} = I_7$, $\frac{r_2}{u} = I_6$ and $x_2 = I_4$, they are checked by Magma. See [5]. ∎

Set

$$M := \begin{pmatrix} z_2 & -z_1 \\ -qz_2 & -(qz_1 + (2a+1)z_2) \end{pmatrix} \in M_2(\mathbb{Z}).$$

By Lemma 5.6, we have that $\det M \cdot (\frac{r_1}{u}, \frac{r_2}{u}) \in \mathbb{Z}^2$, i.e.,

$$(2qz_1z_2 + (2a+1)z_2^2)\left(\frac{r_1}{u},\ \frac{r_2}{u}\right) \in \mathbb{Z}^2. \tag{5.9}$$

Since $u^2 = qz_1^2 + (2a+1)z_1z_2 + kz_2^2$, we also have that

$$(qz_1^2 + (2a+1)z_1z_2 + kz_2^2)\left(\frac{r_1}{u},\ \frac{r_2}{u}\right) \in \mathbb{Z}^2. \tag{5.10}$$

Lemma 5.7. *Set $R := pq^3$. Then it holds that for any coprime integers Z_1, Z_2,*

$$\gcd(qZ_1^2 + (2a+1)Z_1Z_2 + kZ_2^2,\ 2qZ_1Z_2 + (2a+1)Z_2^2) \mid R.$$

Proof. We follow the proof of (a) of Lemma 3′ in [9] (p. 72). Since $a^2 + a + \frac{p+1}{4} = qk$, we have that

$$\frac{4q}{p}(qX^2 + (2a+1)X + k) - \frac{4q}{p}\left(\frac{1}{2}X + \frac{2a+1}{4q}\right)(2qX + (2a+1)) = 1.$$

Let A, a_0, D and d be the same as they are in the proof in [9]. Then we have that $A = p$, $a_0 = q$, $D = 1$ and $d = 2$. Therefore we get the claim. ■

By (5.9), (5.10) and Lemma 5.7, we have that

$$R\,\frac{r_1}{u},\ R\,\frac{r_2}{u} \in \mathbb{Z}.$$

By multiplying $\left(\frac{R}{u}\right)^2$ on the both sides of the first equation in (5.6), we have that

$$q\left(R\,\frac{r_1}{u}\right)^2 + (2a+1)\left(R\,\frac{r_1}{u}\right)\left(R\,\frac{r_2}{u}\right) + k\left(R\,\frac{r_2}{u}\right)^2 + R^2\,\frac{t}{u} + \frac{R^2}{u^2} = 0. \tag{5.11}$$

By using $y_1 = I_3$, $y_2 = I_2$ and $t = I_8u$, we have the following:

Lemma 5.8. *It holds that $y_1 = \frac{t}{u}z_1$, $y_2 = \frac{t}{u}z_2$.*

Proof. It is checked by Magma. See [5]. ■

Since z_1 and z_2 are coprime, we have that $\frac{t}{u} \in \mathbb{Z}$ by Lemma 5.8. Therefore, by (5.11), we have that

$$u^2 = qz_1^2 + (2a+1)z_1z_2 + kz_2^2 \mid R^2 = p^2q^6. \tag{5.12}$$

Lemma 5.9. *We have that $q \nmid u$.*

Proof. Assume that $q|u$. Since $s = -u$, we have that $s \equiv 0 \pmod{q}$. The first and nth equations in (5.6) ($n = 9,\ 10$) imply the following congruence relations:

- $(2a+1)r_1r_2 + kr_2^2 + 1 \equiv 0 \pmod{q}$; (5.13)
- $r_1z_2 \equiv r_2z_1 \pmod{q}$; (5.14)
- $ar_1z_2 + (a+1)r_2z_1 + kr_2z_2 \equiv 0 \pmod{q}$. (5.15)

By (5.14) and (5.15), we have that

$$r_2((2a+1)z_1 + kz_2) \equiv 0 \pmod{q}.$$

By (5.13), we have that $r_2 \not\equiv 0 \pmod{q}$. Therefore

$$(2a+1)z_1 + kz_2 \equiv 0 \pmod{q}. \tag{5.16}$$

By (5.14) and (5.16), we have that

$$\begin{pmatrix} r_2 & -r_1 \\ 2a+1 & k \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{q}.$$

Since z_1 and z_2 are coprime, $(z_1, z_2) \not\equiv (0, 0) \pmod{q}$. Therefore the determinant of the matrix is congruent to 0, i.e., $kr_2 + (2a+1)r_1 \equiv 0 \pmod{q}$. Therefore we have that

$$kr_2^2 + (2a+1)r_1r_2 \equiv 0 \pmod{q}. \tag{5.17}$$

By (5.13) and (5.17), we obtain that $1 \equiv 0 \pmod{q}$. This is a contradiction. ■

By (5.12) and Lemma 5.9, it holds that $qz_1^2 + (2a+1)z_1z_2 + kz_2^2 = 1$ or p^2. Suppose that $qz_1^2 + (2a+1)z_1z_2 + kz_2^2 = p^2$. Since

$$N_{\mathcal{K}/\mathbb{Q}}(z_1q + z_2(a+\omega)) = q(qz_1^2 + (2a+1)z_1z_2 + kz_2^2),$$

the principal ideal (p) (in $\overline{\mathcal{R}}$) divides the principal ideal $(z_1q + z_2(a+\omega))$. In particular $z_1q + z_2(a+\omega) \in \mathbb{Z}p + \mathbb{Z}p\omega$, hence $p|z_1$ and $p|z_2$. This is a contradiction. Therefore we have that

$$N_{\mathcal{K}/\mathbb{Q}}(z_1q + z_2(a+\omega)) = q,$$

i.e., $\overline{\mathfrak{q}} = (z_1q + z_2(a+\omega))$. Hence $\mathfrak{q}$ is also principal. This completes the proof of Theorem 5.1.

Altogether we have the following:

Theorem 5.10. *Let*

$$\begin{aligned} E &: y^2 = x^3 + (i-2)x^2 + x, \\ A &: y^2 = x^3 - x, \\ C &: y^2 = x^5 + 16x^4 - 8x^3 - 64x^2 + 16x \end{aligned}$$

be the curves defined over $\mathbb{Q}(i)$, $\mathbb{Q}$ and $\mathbb{Q}$, respectively. Then, for any prime number p, the following conditions are equivalent:

(1) *there exists a supersingular prime ideal of E lying over p;*
(2) $p \equiv 3 \pmod 4$ *and $J(C)_p$ is isomorphic to $A_p \times A_p$ over $\mathbb{F}_{p^2}$;*
(3) $p \equiv 3 \pmod 4$ *and $J(C)_p$ is isomorphic to $A_p \times A_p$ over $\mathbb{F}_p$.*

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[2] N.D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. math. **89** (1987), 561–567.

[3] T. Ibukiyama, T. Katsura and F. Oort, *Supersingular curves of genus two and class numbers*, Compos. Math. **57** (1986), 127–152.

[4] D. Mumford, *Abelian Varieties*, 2nd ed., Oxford Univ. Press (1974).

[5] N. Murabayashi, *On Magma's commands to solve the simultaneous equations* (5.6), https://drive.google.com/file/d/1vgH8XnTRpbvaXkEUC8WD_K-Aye7zphsF/view?usp=sharing

[6] F. Oort, *Which abelian surfaces are products of elliptic curves?*, Math. Ann. **214** (1975), 35–47.

[7] T. Shioda, *Supersingular $K3$ surfaces, in "Algebraic Geometry"*, Springer Lecture Notes **732** (1978), 564–591.

[8] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, New York (1986).

[9] J.H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York (1992).

[10] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[11] C.F. Yu, *Superspecial abelian varieties over finite fields*, J. Pure Appl. Algebra **216** (2012), 1418−1427.

Address: Naoki Murabayashi: Department of Mathematics, Faculty of Engineering Science, Kansai University, 3-3-35, Yamate-cho, Suita-shi, Osaka, 564-8680, Japan.

E-mail: murabaya@kansai-u.ac.jp

Received: 22 February 2017; **revised:** 6 January 2018