Computations on the Deuring Correspondence of Supersingular Elliptic Curves

Chung Ying Li

1. Introduction

Let $E/F_p^2$ be a supersingular elliptic curve, where $p$ is a prime. It is known that $\text{End}_{F_p}(E)$ is isomorphic to a maximal order of $\mathbb{Q}_{p,\infty}$, the quaternion algebra over $\mathbb{Q}$ ramified at $p$ and $\infty$. By Deuring’s Theorem, there is a 1-1 correspondence between supersingular elliptic curves $E/F_p^2$ and maximal orders of $\mathbb{Q}_{p,\infty}$. But for a given list of supersingular $j$-invariants, in practice, we do not immediately obtain the corresponding maximal orders of $\mathbb{Q}_{p,\infty}$. In this master thesis, we intend to discuss a computation method that leads to realize the Deuring correspondence. After reviewing the basic theory of supersingular elliptic curves in Section 2, we begin to study the construction of isogeny and endomorphism rings in Section 3, where computations of a few examples were included. Finally, after summarizing the results of Deuring, Pizer, we match the endomorphism rings and the maximal orders according to Deuring’s Correspondence.

2. Preliminaries

An elliptic curve $E$ over a perfect field $K$ is a smooth curve of genus 1 having a specified basepoint $O$. We usually write it with the Weierstrass equation as an equation to the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, \cdots, a_6 \in K$ and plus the point $O = [0, 1, 0]$ at infinity. If char$(K) \neq 2$, then we can simplify the equation to the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where $b_2 = a_1^2 + 4a_2, b_4 = 2a_1 + a_1a_3, b_6 = a_3^2 + 4a_6$. We also define quantities

$b_2 = a_1^2 + 4a_2, b_4 = 2a_1 + a_1a_3, b_6 = a_3^2 + 4a_6, b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$

$c_4 = b_2^2 - 24b_4, \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ and $j = c_4^3/\Delta$.

It is a basic fact that $j$ is an invariant of the isomorphism class of the given elliptic curve $E$, usually we called the $j$-invariant of $E$.

**Definition 2.1**: If char$(K) \neq 2$, a Weierstrass equation is a Legendre form if it can be written as

$$y^2 = x(x - 1)(x - \lambda), \text{ where } \lambda \in K.$$
Proposition 2.2: Assume \( \text{char}(K) \neq 2 \).

1. Every elliptic curve \( E/K \) is isomorphic (over \( \overline{K} \)) to an elliptic curve in Legendre form
   \[
   E_\lambda : y^2 = x(x-1)(x-\lambda)
   \]
   for some \( \lambda \in \overline{K}, \lambda \neq 0, 1 \)
2. The \( j \)-invariant of \( E_\lambda \) is
   \[
   j(E_\lambda) = \frac{28(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.
   \]

Proof: see Ch.3 [Sil].

Composition Law 2.2: Let \( P, Q \in E \), \( L \) be a line connecting \( P, Q \) (tangent line if \( P = Q \)), and \( R \) be the third point of intersection of \( E \) and \( L \). Let \( L' \) be the line connecting \( R \) and \( O \). Then \( P \oplus Q \) is the point such that \( L' \) intersects \( E \) at \( R, O \) and \( P \oplus Q \).

Proposition 2.3: \((E, \oplus)\) forms an abelian group with identity element \( O \).

Proof: see Ch.3 [Sil].

Notation 2.4: \( m \in \mathbb{Z}, \ P_0 = (x_0, y_0) \in E \), we define

1. \([m]P_0 = P_0 \oplus \cdots \oplus P_0 \) \( (m \) times), where \( m > 0 \)
2. \([0]P_0 = O \)
3. \([-m]P_0 = (-P_0) \oplus \cdots \oplus (-P_0) \), where \( m < 0 \)

We can calculate the point \(-P_0 = (x_0, -y_0 - a_1x_0 - a_3)\), and

\[
\quad x([2]P_0) = \frac{x_0^4 - b_4x_0^2 - 2b_6x_0 - b_8}{4x_0^3 + b_2x_0^2 + b_4x_0 + b_6}.
\]

For convenience, we usually use "+" instead of "\( \oplus \)".
Definition 2.5: Let $E_1$ and $E_2$ be two elliptic curves. An isogeny between $E_1$ and $E_2$ is a morphism $\phi : E_1 \to E_2$ such that $\phi(O) = O$. $E_1$ and $E_2$ are isogenous if there is an isogeny $\phi$ such that $\phi(E_1) \neq O$. In fact, a morphism from $E_1$ and $E_2$ is either a constant or a surjective map.

Now, let $E_1/K$ and $E_2/K$ be two elliptic curves and let $\phi : E_1 \to E_2$ be a non-constant rational map defined over $K$. Then $\phi$ induces an injection of function fields fixed $K$,

$$\phi^* : K(E_2) \to K(E_1)$$

$$\phi^* f = f \circ \phi$$

where $f$ is a rational map.

Theorem 2.6: Let $E_1/K$ and $E_2/K$ be two elliptic curves. If $\phi : E_1 \to E_2$ is a non-constant rational map defined on $K$, then $K(E_1)$ is a finite extension of $\phi^* K(E_2)$.

Proof: see Ch.2 [Sil].

If $\phi : E_1 \to E_2$ is a nonzero isogeny over $K$ and $\phi^* : K(E_2) \to K(E_1)$ is the induced map, we define $\deg \phi = \deg K(E_1)/\phi^* K(E_2)$. Let $\deg_s \phi$ be the separable degree of $\phi$ and let $\deg_i \phi$ be the purely inseparable degree of $\phi$. Set $\deg[0] = 0$. Since elliptic curves are group, the isogenies between them form a group. Let $\text{Hom}(E_1, E_2) = \{\text{isogenies } \phi : E_1 \to E_2\}$ and $\text{End}(E) = \text{Hom}(E, E)$.

Definition 2.7: Let $E$ be an elliptic curve and Let $m \in \mathbb{Z}$. Define the multiplication by $m$,

$$[m] : E \to E$$

$$P \mapsto [m]P.$$ 

If $m \neq 0$, the $m$-torsion subgroup of $E$, denoted by $E[m]$, is the set of $m$-torsion points of $E$. Namely, $E[m] = \{P \in E \mid [m]P = O\}$.

Theorem 2.8: Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree $m$. Then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying

$$\hat{\phi} \circ \phi = [m]$$

Proof: see Ch.3 [Sil].

We call $\hat{\phi}$ the dual isogeny of $\phi$. 

3
**Theorem 2.9**: Let $\phi : E_1 \to E_2$ be an isogeny. Then

\[
\hat{\phi} \circ \phi = [m] \text{ on } E_1,
\]

\[
\phi \circ \hat{\phi} = [m] \text{ on } E_2.
\]

**Proof**: see Ch.3 [Sil].

**Corollary 2.10**: Let $E$ be an elliptic curve, $m \in \mathbb{Z}, m \neq 0$.

1. $\deg[m] = m^2$,

2. If $\text{char}(K) = 0$ or $(m, \text{char}(K)) = 1$, then

\[
E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}),
\]

3. If $\text{char}(K) = p$, then either

\[
E[p^e] \cong 0 \quad \text{for all } e = 1, 2, \cdots \quad \text{or}
\]

\[
E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \quad \text{for all } e = 1, 2, \cdots.
\]

**Proof**: see Ch.3 [Sil].

Now, we recall some well-known results on elliptic curve over a perfect field $K$ of characteristic $p$.

**Theorem 2.11**: Let $E/K$ an elliptic curve. For each integer $r \geq 1$, let

\[
\phi_r : E \to E^{(p^r)} \quad \text{and} \quad \hat{\phi}_r : E^{(p^r)} \to E
\]

be the $p^r$-power Frobenius map and its dual. The followings are equivalent:

1. $E[p^r] = 0$ for one (all) $r \geq 1$.

2. $\hat{\phi}_r$ is (purely) inseparable for one (all) $r \geq 1$.

3. The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.

4. $\text{End}(E)$ is an order in a quaternion algebra. (Note $\text{End}(E)$ means $\text{End}_{\mathcal{O}}(E)$)

5. The formal group $\hat{E}/K$ associated to $E$ has height 2.

**Proof**: see Ch.5 [Sil].
**Definition 2.12**: $E$ is *supersingular* (or has *Hasse invariant* 0) if it satisfies the equivalent conditions on Theorem 2.11, otherwise $E$ is ordinary (or has *Hasse invariant* 1).

There are only finitely many (up to isomorphism) elliptic curves with *Hasse invariant* 0, since each $j$-invariant is in $\mathbb{F}_p^2$. The following result is well-known.

**Theorem 2.13**: Let $K$ be a finite field of characteristic $p$.

1. If $p = 2$, then the only *supersingular* elliptic curve is $E : y^2 + y = x^3$.
2. If $p > 2$ and let $E/K$ be an elliptic curve with Weierstrass equation

   $$E : y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6$$

   with distinct roots (in $\overline{K}$). Then $E$ is *supersingular* if and only if the coefficient of $x^{p-1}$ in $f(x)^{(p-1)/2}$ is zero.
3. Let $m = \frac{p-1}{2}$ and define a polynomial

   $$H_p(t) = \sum_{i=0}^{m} \left( \frac{m}{i} \right)^2 t^i.$$ 

   Let $\lambda \in \overline{K}$, $\lambda \neq 0,1$. Then the elliptic curve

   $$E : y^2 = x(x-1)(x-\lambda)$$

   is *supersingular* if and only if $H_p(\lambda) = 0$.
4. The polynomial $H_p(t)$ has distinct roots in $\overline{K}$. Up to isomorphism, there are exactly

   $$\left[ \frac{p}{12} \right] + \epsilon_p$$

   *supersingular* elliptic curves in characteristic $p$, where $\epsilon_3 = 1$, and for $p \geq 5$,

   $$\epsilon_p = 0, 1, 1, 2 \quad \text{if} \quad p \equiv 1, 5, 7, 11 \pmod{12}$$

**Proof**: see Ch.5 [Sil].
3 Isogeny Construction

In this section, we construct the canonical quotient map \( \phi : E \to E/C \), where \( E/K \) is an elliptic curve and \( C \subseteq E \) is a cyclic subgroup of order \( n \). We show that how to choose Weierstrass parameter on \( E/C \) (by choosing their pullback to \( E \)) and compute the resulting Weierstrass equation.

For the purpose of this thesis, we restrict the case to the supersingular elliptic curve \( E/F_{p^2} \). Then every separable isogeny of \( E \) can be factored into cyclic isogenies of prime degree \( n \neq p \). Thus let \( C \) runs through all possible cyclic subgroups, and compute the \( j \)-invariant from the Weierstrass equation, we can conclude the representation numbers, i.e., the number of endomorphisms of \( E \) with degree \( n \) for each \( n \). We deal with the \( n = 2 \) and \( n > 2 \) cases separately.

3.1 Case 1: \( n = 2 \)

Let \( p \neq 2 \), we choose a Weierstrass equation for \( E \) to be of the form

\[
y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = x^3 + a_2x^2 + a_4x + a_6.
\]

Then the three cyclic subgroups of order 2 which serve as the kernel of a degree 2 isogeny are given by \( C_i = \langle (\alpha_i, 0) \rangle, i = 1, 2, 3 \). The following proposition shows that how to choose a degree 2 Weierstrass parameter on \( E/C_i \). Without loss of generality, let us assume that \( C = C_1 \).

**Proposition 3.1:** Let \( C = \langle (\alpha_1, 0) \rangle \) and let \( \phi : E \to E/C \) be the canonical quotient map. Then there is a function \( t \in L(2(\infty)) \) on \( E/C \) with

\[
\phi^* t = \frac{(x - \alpha_2)(x - \alpha_3)}{(x - \alpha_1)}
\]

**Proof:** Let \( P_i = (\alpha_i, 0) \) for each \( i \) and let \( \phi(P_i) = P_i \) in \( E/C \). Since \( P_2 \) is not in \( \text{Ker}\phi \) and \( P_2 \) has order 2, so \( P_2 \) has order 2 in \( E/C \). Then there exists a function \( f \in E/C \) such that

\[
\text{div}(f) = 2P_2 - 2(\infty)
\]

We have \( P_1 + P_2 = -P_3 = P_3 \). The preimage of \( P_2 \) consists of \( P_2 \) and \( P_2 + P_1 (= P_3) \).

By \( \sum_{P \in \phi^{-1}(P_2)} e_\phi(P) = \deg(\phi) = 2 \), it yields that \( e_\phi(P_3) = 1 \) and \( e_\phi(P_2) = 1 \), and

\[
\text{div}(\phi^* f) = 2(e_\phi(P_2)P_2 + e_\phi(P_3)P_3) - 2(e_\phi(P_1)P_1 + e_\phi(\infty)\infty) \\
= 2P_2 + 2P_3 - 2P_1 - 2(\infty).
\]

Thus

\[
\phi^* f = \frac{c_2(x - \alpha_2)c_3(x - \alpha_3)}{c_1(x - \alpha_1)}
\]
for some nonzero constants \(c_1, c_2\) and \(c_3\). Take \(t = (c_1/c_2c_3)f\), we have the assertion.

On the curve \(E/C\), we now have a function \(t \in L(2(\infty))\). Furthermore, \(t\) vanishes at one point of order 2, namely \(P_2\). Therefore there must be a function \(z \in L(3(\infty))\) such that \(E/C\) has the following Weierstrass equation

\[
z^2 = t(t - t_1)(t - t_2)
\]

It is clearly that \(t_1\) and \(t_2\) are the other points of order 2 on \(E/C\). These two points are precisely the images under \(\phi\) of the four points which satisfy the equation 

\[\[2\]Q = P_1\] in \(E\). Therefore we may find a Weierstrass equation for \(E/C\) by solving \(\[2\]Q = P_1\) and evaluating \(\phi^*t\) at these points.

**Proposition 3.2**: Let \(Q_1\) and \(Q_2\) be two points in \(E\) with \(\[2\]Q_i = P_1\), \(i = 1, 2\) and let \(Q_2 \neq -Q_1\). Then \(E/C\) has the Weierstrass equation

\[
z^2 = t(t - t_1)(t - t_2), \text{ where } t_i = \phi^*t(Q_i), i = 1, 2.
\]

**Proof**: Note that \(Q_1 + Q_1 + P_1 + P_1 = 0, Q_2 + Q_2 + P_1 + P_1 = 0\) and \(-Q_1 \neq Q_2\). So, \(Q_1 + Q_2 \neq 0\) implies \(Q_2 \neq Q_1 + P_1\). Thus \(Q_1\) and \(Q_2\) have distinct images in \(E/C\). Our assertion follows from the above discussion.

**Remark 3.3**: The \(x\)-coordinates of the points \(Q_1\) and \(Q_2\) satisfies the duplication formula

\[
x((2)Q) = \frac{x_0^4 - b_4x_0^2 - 2b_6x_0 - b_8}{4x_0^3 + b_2x_0^2 + 2b_4x_0 + b_6} = \alpha_1.
\]

This equation have precisely two roots, \(x_1 = x(Q_1)\) and \(x_2 = x(Q_2)\). We can substitute them into the formula for \(\phi^*t\) to find \(t_1\) and \(t_2\).

**Example 1**: Choose the followings supersingular elliptic curve with \(j\)-invariant 0 in characteristic \(p = 41\),

\[E : y^2 = x^3 + x^2 + 14x = x(x - (20 + 7\sqrt{-3}))(x - (20 + 34\sqrt{-3}))\]

Take \(C_1 = <(0, 0)>, \text{ and let } \frac{t(x)}{x} = \frac{x^2 + x + 14}{x}, \text{ then the } x\)-coordinates of \(Q_1\) and \(Q_2\) satisfy the equation

\[
x((2)Q) = \frac{x^4 - 28x^2 + 32}{4(x^3 + x^2 + 14x)} = 0.
\]

Then \(x_1 = 3\sqrt{-3}\) and \(x_2 = 38\sqrt{-3}\). It yields \(t_1 = 1 + 6\sqrt{-3}\) and \(t_2 = 1 + 35\sqrt{-3}\). Therefore, the Weierstrass equation for \(E/C_{11}\) is

\[
z^2 = t^3 + 39t^2 + 27t
\]
and $j$-invariant of $E/C$ is 3.

\[ \square \]

3.2 Case 2: $n \geq 3$

We still take $n$ to be a prime. For simplicity, let the Weierstrass equation for $E$ be the form

\[ E : y^2 = x(x - \alpha_1)(x - \alpha_2) = x^3 + a_2x^2 + a_4x. \]

Then $(0,0)$ is order 2. Let $C \subseteq E$ be a cyclic subgroup of order $n$, generated by a point $P$. As in Case 1, we will find a degree 2 function $t \in L(2(\infty))$ on $E/C$.

**Proposition 3.4**: Let $\phi : E \to E/C$ be the canonical quotient map. For each $1 \leq i \leq n-1$, let $P_i = [i]P$ and $Q_i = (0,0) + P_i$. Then there is a degree 2 function $t \in L(2(\infty))$ on $E/C$ with

\[ \phi^*t = x \prod_{i=1}^{n-1} \left( \frac{x - x(Q_i)}{x - x(P_i)} \right) = x \prod_{i=1}^{n-1} \left( \frac{x - x(Q_i)}{x - x(P_i)} \right)^2 \]

**Proof**: From Proposition 3.1, $(0,0)$ is a point of order 2 which is not in $\ker(\phi)$, then there exists a function $s \in E/C$ such that

\[ \text{div}(s) = 2(0,0) - 2(\infty) \]

Since the preimage of $\infty$ is exactly $C$, then the inverse image of $(0,0)$ is the coset $(0,0) + C$ exactly. So

\[ \text{div}(\phi^*s) = 2(\sum_{P \in \phi^{-1}(0,0)} e_\phi(P)P) - 2(\sum_{P \in \phi^{-1}(\infty)} e_\phi(P)P) \]

\[ = 2(0,0) + 2Q_1 + \cdots + 2Q_{n-1} - 2(\infty) - 2P_1 - \cdots - 2P_{n-1} \]

Compare the divisors,

\[ P_{n-i} = [n-i]P = [-i]P = -P_i, \]

\[ Q_{n-i} = (0,0) + [n-i]P = -((0,0) + [i]P) = -Q_i, \]

We know that $\text{div}(x) = 2(0,0) - 2(\infty)$, so

\[ \text{div}(x - x(P_i)) = P_i + (-P_i) - 2(\infty) = P_i + P_{n-i} - 2(\infty) \text{ and} \]

\[ \text{div}(x - x(Q_i)) = Q_i + Q_{n-i} - 2(\infty). \]

Thus,

\[ 2(0,0) + 2Q_1 + \cdots + 2Q_{n-i} - 2(\infty) - 2P_1 - \cdots - 2P_{n-i} \]
\[\text{div} \left( \frac{n-1}{x} \prod_{i=1}^{n-1} \left( \frac{x - x(Q_i)}{x - x(P_i)} \right)^2 \right)\]

**Proposition 3.5**: Let \( t_1 = \phi^* t(\alpha_1,0) \) and \( t_2 = \phi^* t(\alpha_2,0) \) as above. Then \( E/C \) has the Weierstrass equation
\[z^2 = t(t - t_1)(t - t_2)\]

**proof**: As Proposition 3.2, There are three points, \((0,0)\), \((\alpha_1,0)\) and \((\alpha_2,0)\) that their images are of order 2 on \( E/C \); \( t \) has chosen to vanish at \((0,0)\).

**Remark 3.6**: Since \( Q_i = (0,0) + P_i \), each \( x(Q_i) \) can be computed from the corresponding \( x(P_i) \). If we let \( P_i = (x_i, y_i) \), the line through \((0,0)\) and \( P_i \) is given by the equation \( y = \frac{y_i}{x_i} x \). To compute \( x(Q_i) \), we substitute it into the Weierstrass equation for \( E \) and obtain
\[\frac{y_i}{x_i} x^2 = x^3 + a_2 x^2 + a_4 x\]
\[\frac{x_i^3 + a_2 x_i^2 + a_4 x_i x^2}{x_i^2} = x^3 + a_2 x^2 + a_4 x\]
\[0 = x^3 - (x_i + \frac{a_4}{x_i}) x^2 + a_4 x\]
\[0 = x(x - x_i)(x - \frac{a_4}{x_i})\]
Thus \( x(Q_i) = a_4 / x_i \).

**Example 2**: First, we compute the isogeny of degree 3 for the curve in Example 1.
\[E : y^2 = x^3 + x^2 + 14x = x(x - (20 + 7\sqrt{-3}))(x - (20 + 34\sqrt{-3}))\]
To find the group of order 3, we solve the equation
\[x([2]Q) = \frac{x^4 - 28x^2 + 196}{4(x^3 + x^2 + 14x)} = x\]
\[38(14 + x)(33 + x)(4 + 9x + x^2) = 0\]
Take \( x_1 = -14 \), then the function \( x(Q) = \frac{a_4}{x_1} = \frac{14}{-14} = 40 \). It yields
\[t(x) = \frac{x(x - 40)^2}{(x + 14)^2}, \quad t_i = t(20 \pm 7\sqrt{-3}) = 22 \pm 20\sqrt{-3}, \quad i = 1, 2.\]
Then the Weierstrass equation for \( E/C \) is
\[z^2 = t^3 + 38t^2 + 3t\]
and the $j$-invariant for $E/C$ is 0.

Next, we compute the Weierstrass equation for elliptic curve $E/C$, where $C$ is a cyclic group of order 5. First, compute $x([4]P) = x$ and dividing out the 3-torsion polynomial, we have the following polynomial whose roots are the $x$-coordinates of points of order 5 on $E$.

$$(34 + x^2 + 12x + x^2)(34 + 14x + x^2)(35 + 17x + x^2)(26 + 18x + x^2)(28 + 24x + x^2) = 0$$

Take $x(P_1) = 20 + 3\sqrt{-3}$. Then $x(P_2) = 29 + 4\sqrt{-3}$. It yields $x(Q_1) = a_4/x(P_1) = 1 + 2\sqrt{-3}$ and $x(Q_2) = 35 + 39\sqrt{-3}$. So

$$t(x) = \frac{x(x - (1 + 2\sqrt{-3}))^2(x - (35 + 39\sqrt{-3})^2}{(x - (20 + 3\sqrt{-3})^2(x - (29 + 4\sqrt{-3}))^2}.$$ Thus

$$t_1 = t(20 + 7\sqrt{-3}) = 3 + 19\sqrt{-3} 	ext{ and } t_2 = t(20 + 34\sqrt{-3}) = 33 + 11\sqrt{-3}.$$

We obtain the Weierstrass equation of $E/C$ which is

$$z^2 = t^3 + (5 + 11\sqrt{-3})t^2 + (5 + 4\sqrt{-3})t$$

and the $j$-invariant for $E/C$ is -13.

\[\square\]

### 3.3 Explicit Generators of $\text{End}_{\mathbb{F}_p^2}(E)$

In this section, we will compute the endomorphism ring of $E$. In previous examples, we compute the canonical quotient map from $E$ to $E/C$ for some subgroup $C$ of $E$, this determines whether there is an endomorphism of $E$ with Kernel $C$. If there is one, then we could choose an isomorphism $\gamma : E \to E/C$, so that $\gamma^{-1} \circ \phi : E \to E/C \to E$ is an endomorphism of $E$ with kernel $C$.

**Proposition 3.7**: The function $z$ in Proposition 3.2 can be chosen as

$$\phi^* z = \frac{(x - x(Q_1))(x - x(Q_2))y}{(x - \alpha_1)^2}.$$

**Proof**: From the proof of Proposition 3.1, on $E/C$ we have

$$\text{div}(\phi^* z) = P_2 + P_3 + Q_1 + (-Q_1) + Q_2 + (-Q_2) - 3P_1 - 3(\infty)$$

We also know the divisors on $E$:

$$\text{div}(y) = P_1 + P_2 + P_3 - 3(\infty)$$

$$\text{div}(x - x(Q_i)) = Q_i + (-Q_i) - 2(\infty)$$

So,

$$\phi^* z = M \frac{(x - x(Q_1))(x - x(Q_2))y}{(x - \alpha_1)^2}$$

10
for some nonzero constant $M$. Substitute this expression for $z$ and the expression for $t$ into the equation $z^2 = t(t - t_1)(t - t_2)$, we obtain an equation in $x$ and $y$. Then replacing $y^2$ with $x^3 + a_2x^2 + a_4x + a_6$, we obtain a polynomial in $x$ with leading coefficient $M^2 - 1$. So $M$ is 1 or -1.

Proposition 3.8: The function $z$ in Proposition 3.5 can be chosen so that

$$\phi^* z = y \prod_{i=1}^{n-1} \frac{(x - x(Q_i))(x - x(R_i))(x - x(S_i))}{(x - x(P_i))^3},$$

where $P_i = [i]P$, $Q_i = (0, 0) + P_i$, $R_i = (\alpha_1, 0) + P_i$, $S_i = (\alpha_2, 0) + P_i$.

Proof: From the proof of Proposition 3.5, the divisor of $z$ on $E/C$ is

$$\text{div}(z) = (0, 0) + (\alpha_1, 0) + (\alpha_2, 0) - 3(\infty).$$

Therefore the divisor of $\phi^* z$ on $E$ is

$$(0, 0) + (\alpha_1, 0) + (\alpha_2, 0) + \sum_{i=1}^{n-1} ((Q_i) + (R_i) + (S_i)) - 3(\infty) - 3 \sum_{i=1}^{n-1} (P_i).$$

Similarly, we have the following divisors on $E$ to work with:

$$P_{n-i} = -P_i \implies \text{div}(x - x(P_i)) = P_i + P_{n-i} - 2(\infty),$$

$$Q_{n-i} = -Q_i \implies \text{div}(x - x(Q_i)) = Q_i + Q_{n-i} - 2(\infty),$$

$$R_{n-i} = -R_i \implies \text{div}(x - x(R_i)) = R_i + R_{n-i} - 2(\infty),$$

$$S_{n-i} = -S_i \implies \text{div}(x - x(S_i)) = S_i + S_{n-i} - 2(\infty).$$

We know $\text{div}(y) = (0, 0) + (\alpha_1, 0) + (\alpha_2, 0) - 3(\infty)$. It yields

$$\phi^* z = M \frac{(x - x(Q_i))(x - x(R_i))(x - x(S_i))y}{(x - x(P_i))^3}$$

for some nonzero constant $M$. As in the previous proposition, substitute this and the formula for $t$ into the Weierstrass equation for $E/C$, resulting in a polynomial in $x$ whose leading coefficient is $M^2 - 1$. So $M$ is 1 or -1.

Proposition 3.9: Let

$$E_1 : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

$$E_2 : z^2 = t(t - t_1)(t - t_2)$$
Then, up to reordering of the $\alpha$’s, every isomorphism $\gamma : E_1 \to E_2$ is given by
\[
(t, z) = \gamma(x, y) = (\beta^2(x - \alpha_1), \pm \beta^3y)
\]
with
\[
\beta^2 = \frac{t_1}{\alpha_2 - \alpha_1} = \frac{t_2}{\alpha_3 - \alpha_1}.
\]

**Proof**: $\gamma^{-1}(0, 0)$ must be a point of order 2, we can renumber as $(\alpha_1, 0)$. So that $(\alpha_1, 0)$ sends to $(0, 0)$, $(\alpha_2, 0)$ sends to $(t_1, 0)$, and $(\alpha_3, 0)$ sends to $(t_2, 0)$. Therefore, $\text{div}(\gamma^*t) = 2(\alpha_1, 0) - 2(\infty)$. By Comparison of divisors, we have $\gamma^*t = \beta^2(x - \alpha_1)$, where $\beta^2$ satisfies the stated condition.

Finally,
\[
\gamma^*(z^2) = \gamma^*(t(t - t_1)(t - t_2))
\]
\[
= \beta^2(x - \alpha_1)(\beta^2(x - \alpha_1) - t_1)(\beta^2(x - \alpha_1) - t_2)
\]
\[
= \beta^2(x - \alpha_1)(\beta^2(x - \alpha_1) - \beta^2(\alpha_2 - \alpha_1))(\beta^2(x - \alpha_1) - \beta^2(\alpha_3 - \alpha_1))
\]
\[
= \beta^6(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)
\]
\[
\implies \gamma^*z = \pm \beta^3y.
\]

\[\square\]

**Corollary 3.10**: Once an explicit formula for $\phi : E \to E/C$ has been found, there are twelve maps to check, in order to determine a complete set of endomorphisms $\gamma^{-1} \circ \phi : E \to E$ with kernel $C$.

**Example 4**: Let $E : y^2 = x^3 + x^2 + 14x = x(x - (20 + 7\sqrt{-3}))(x - (20 + 34\sqrt{-3}))$ in characteristic $p = 41$. $C = \langle P \rangle$ is the group of order 3 as in Example 2. Then we obtain $E/C : z^2 = t^3 + 38t^2 + 3t = t(t - (22 + 20\sqrt{-3}))(t - (22 + 21\sqrt{-3}))$. Substitute $0, 20 + 7\sqrt{-3}$, and $20 + 34\sqrt{-3}$ for $\alpha$’s and $22 + 20\sqrt{-3}$ and $22 + 21\sqrt{-3}$ for $t$’s. We check them by Proposition 3.9 and obtain 6 endomorphisms of $E$ with kernel $C$, given by $\gamma^{-1} \circ \phi$.

In the following, we list the table of the number of endomorphisms of $E$ with kernel of degree $i$, $i = 1, 2, 3$ and 5 for four different *supersingular* elliptic curves in characteristic $p = 41$. 

---

12
\( j = 0, \quad E: y^2 = x^3 + x^2 + 14x \)

<table>
<thead>
<tr>
<th>( C )</th>
<th>( j )-invariant</th>
<th>endomorphism</th>
</tr>
</thead>
<tbody>
<tr>
<td>( &lt; (0,0) &gt; )</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>( &lt; (20 + 7\sqrt{-3},0) &gt; )</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>( &lt; (20 + 34\sqrt{-3},0) &gt; )</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Degree 2 Isogenies from \( j = 0 \) over \( \mathbb{F}_{41} \)

<table>
<thead>
<tr>
<th>( x(P_1) )</th>
<th>( j )-invariant</th>
<th>endomorphism</th>
</tr>
</thead>
<tbody>
<tr>
<td>-14</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>-33</td>
<td>-13</td>
<td>0</td>
</tr>
<tr>
<td>16 + 11\sqrt{-3}</td>
<td>-13</td>
<td>0</td>
</tr>
<tr>
<td>16 + 30\sqrt{-3}</td>
<td>-13</td>
<td>0</td>
</tr>
</tbody>
</table>

Degree 3 Isogenies from \( j = 0 \) over \( \mathbb{F}_{41} \)

<table>
<thead>
<tr>
<th>( x(P_1), x(P_2) )</th>
<th>( j )-invariant</th>
<th>endomorphism</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 + \sqrt{-3}, 29 + 4\sqrt{-3}</td>
<td>-13</td>
<td>0</td>
</tr>
<tr>
<td>20 + 40\sqrt{-3}, 29 + 37\sqrt{-3}</td>
<td>-13</td>
<td>0</td>
</tr>
<tr>
<td>35 + 20\sqrt{-3}, 35 + 21\sqrt{-3}</td>
<td>-9</td>
<td>0</td>
</tr>
<tr>
<td>34 + 6\sqrt{-3}, 12 + 27\sqrt{-3}</td>
<td>-9</td>
<td>0</td>
</tr>
<tr>
<td>34 + 35\sqrt{-3}, 12 + 14\sqrt{-3}</td>
<td>-9</td>
<td>0</td>
</tr>
<tr>
<td>32 + 3\sqrt{-3}, 32 + 38\sqrt{-3}</td>
<td>-13</td>
<td>0</td>
</tr>
</tbody>
</table>

Degree 5 Isogenies from \( j = 0 \) over \( \mathbb{F}_{41} \)

<table>
<thead>
<tr>
<th>( i )</th>
<th>( j = 0 )</th>
<th>( j = 3 )</th>
<th>( j = -9 )</th>
<th>( j = -13 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>2</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

The Number of Endomorphisms of 4 Supersingular Elliptic Curves with Degree \( n \)
4. Matching Endomorphism Rings and Maximal Orders

In this section we review some of the basic theory relating supersingular endomorphism rings and quaternion algebras, mostly due to Deuring. We then describe a method for generating a complete list of representatives $O_i$ for each type of maximal order in $\mathbb{Q}_{p,\infty}$. Based on these representations of the maximal orders, we then offer a straightforward algorithm for computing the so-called representation numbers $(O_i, l)$ which can be used to match each supersingular endomorphism ring with an isomorphic maximal order. Finally, we conclude the section by explicitly computing the first few representation numbers for $p = 41$, and combining this information with that of the previous section to successfully match endomorphism rings with maximal orders in this specific case.

4.1 Background Results of Deuring, Pizer

First, we recall Deuring's Theorem, which establish the connection between isogenies of supersingular elliptic curves and the left ideals of some maximal order of the quaternion algebra $\mathbb{Q}_{p,\infty}$. More detail and proof can be found in [D2, 2.1-2.4,10.2]

**Theorem 4.1 (Deuring)**: Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. Then we have the following:

1. $\text{End}(E)$ is isomorphic to some maximal order $\mathcal{O} = \mathcal{O}_E \subseteq \mathbb{Q}_{p,\infty}$.
2. There is a 1-1 correspondence between left ideals of $\mathcal{O}$ of norm $n$ and isogenies of $E$ of degree $n$.
3. Let $f : E \rightarrow E'$ be an isogeny corresponding to the left ideal $I_f$. Then $\text{End}(E')$ is isomorphic to the right order of $I_f$ in $\text{End}(E) \otimes \mathbb{Q}$, i.e.
   $$\text{End}(E') \cong \mathcal{O}_f := \{ x \in \text{End}(E) \otimes \mathbb{Q} | I_f x \subseteq I_f \}$$
4. Suppose that $f_1 : E \rightarrow E_1$ and $f_2 : E \rightarrow E_2$ are two isogenies corresponding to the left ideals $I_1, I_2 \subseteq \mathcal{O}$. Then
   $$E_1 \cong E_2 \iff I_1 = I_2 x \text{ for some } x \in \text{End}(E) \otimes \mathbb{Q}.$$ 

$\Box$

**Note 4.2**: In statement (2), we count isogenies $f_1 : E \rightarrow E_1$ and $f_2 : E \rightarrow E_2$ as equivalent if $f_1$ and $f_2$ identify the function fields of $E_1$ and $E_2$ with the same subfield of $E$. Also, by $\text{End}(E)$ we will always mean endomorphisms over $\mathbb{F}_p$.

Actually, comparing Eichler’s class number for any maximal order ([D2, 10.3]) with the number of $j$-invariants of supersingular elliptic curves, there can be only
one isogeny class of *supersingular* elliptic curves for a given $p$. Furthermore, for any $\mathcal{O}$, every maximal order type occurs as the right order for some left ideal. Thus, when a maximal order is given, we are choosing the endomorphism ring of a particular *supersingular* elliptic curve. So, the ideal classes of $\mathcal{O}$ are corresponding to all of the *supersingular* elliptic curves.

**Corollary 4.3** (Deuring) : Let $\mathcal{O}$ be any maximal order in $\mathbb{Q}_{p, \infty}$, and let $I_1, \cdots, I_h$ be representatives of the $h$ distinct left-ideal classes, and $\mathcal{O}_i$ be the right order of $I_i$ for each $i$. Then there are $h$ distinct *supersingular* elliptic curves, say $E_1, \cdots, E_h$ such that $\text{End}(E_i) \cong \mathcal{O}_i$. □

**Remark 4.4** : For *supersingular* elliptic curves, Deuring shows in [D2,10.2] that $\text{End}(E_1) \cong \text{End}(E_2)$ and $E_1 \not\cong E_2$ exactly when $j(E_1)$ and $j(E_2)$ are Galois conjugates in $\mathbb{F}_{p^2}$. Equivalently, we see in [P2,2.5] that $\mathcal{O}_i \cong \mathcal{O}_j$ with $i \neq j$ exactly $\mathcal{O}_i$ has a nontrivial two-sided ideal class.

In order to implement of Theorem 4.1, we have to describe the concrete representations for $\mathbb{Q}_{p, \infty}$, a maximal order $\mathcal{O}$, and the right orders $\mathcal{O}_i$ of the left ideal classes representatives $I_1, \cdots, I_h$. The following result is due to Pizer ([P3, 5.1]).

**Theorem 4.5** (Pizer) : The quaternion algebra $\mathbb{Q}_{p, \infty}$ can be written as $\mathbb{Q}[i,j,k]$ with $i^2 = a$, $j^2 = b$, and $ij = -ji = k$, where

- $(a,b) = (-1,-1)$ if $p = 2$,
- $(a,b) = (-1,-p)$ if $p \equiv 3 \pmod{4}$,
- $(a,b) = (-2,-p)$ if $p \equiv 5 \pmod{8}$,
- $(a,b) = (-p,-q)$ if $p \equiv 1 \pmod{8}$,

where $q$ is a prime with $q \equiv 3 \pmod{4}$ and $(p/q) = -1$. □

Pizer goes on in [P2,5.2] to give a basis over $\mathbb{Z}$ for a particular maximal order $\mathcal{O}$ using this same representation. He also offers an algorithm for generating ideal class representatives, specially for computing modular forms ([P3,p.363]). This algorithm is based on the assumption that all left ideals of $\mathcal{O}$ should be induced from an ideal in an imaginary quadratic subfield.

**Note 4.6** : The construction of Theorem 4.5 can be performed in MAGMA with the command QuaternionAlgebra. MAGMA will also choose a maximal order and produce left ideal class representatives, but not with the method outlined in Pizer’s paper. □

From the result of Pizer, we may represent $\mathbb{Q}_{p, \infty}$ as $\mathbb{Q}[i,j,k]$, where $i, j$ and $k$ are as Theorem 4.5. Suppose that $\mathcal{O}$ is any maximal order generated as a module over $\mathbb{Z}$
by the elements $\alpha_1, \ldots, \alpha_4$ with
\[
\begin{bmatrix}
\alpha_1 \\
\alpha_2 \\
\alpha_3 \\
\alpha_4
\end{bmatrix} = \begin{bmatrix}
a_{11} & a_{12} & a_{13} & a_{14} \\
a_{21} & a_{22} & a_{23} & a_{24} \\
a_{31} & a_{32} & a_{33} & a_{34} \\
a_{41} & a_{42} & a_{43} & a_{44}
\end{bmatrix} \begin{bmatrix} 1 \\ i \\ j \\ k \end{bmatrix} = A^T \cdot \begin{bmatrix} 1 \\ i \\ j \\ k \end{bmatrix}.
\]

Let $d$ be the smallest positive integer for which $dA \in \mathbb{Z}^{4 \times 4}$. Then, we have the following.

**Proposition 4.7**: Let $y_1, \ldots, y_4 \in \mathbb{Z}$ be an integral solution of the quadratic form
\[
y_1^2 - ay_2^2 - by_3^2 + aby_4^2 = d^2l,
\]
and suppose that
\[
\begin{bmatrix}
c_1 \\
c_2 \\
c_3 \\
c_4
\end{bmatrix} = \frac{1}{d} A^{-1} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} \in \mathbb{Z}^4.
\]

Then $x = c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 + c_4\alpha_4$ is an element of $\mathcal{O}$ with $N(x) = l$. Furthermore, these are all such elements.

**Proof**: Let $x = c_1\alpha_1 + \cdots + c_4\alpha_4$ for $c_1, \ldots, c_4 \in \mathbb{Z}$ and $N(x) = l$. We see that
\[
x = c_1(a_{11} + a_{12}i + a_{13}j + a_{14}k) + \cdots + c_4(a_{41} + a_{42}i + a_{43}j + a_{44}k)
\]
\[
= (c_1a_{11} + \cdots + c_4a_{41}) + (c_1a_{12} + \cdots + c_4a_{42})i
\]
\[
+ (c_3a_{13} + \cdots + c_4a_{43})j + (c_1a_{14} + \cdots + c_4a_{44})k
\]

We could let $y_1, \ldots, y_4$ be the coefficients with respect to the standard basis. Then $N(x) = l$ implies that $y_1^2 - ay_2^2 - by_3^2 + aby_4^2 = l$. However, there maybe no such $y_1, \ldots, y_4 \in \mathbb{Z}$. Let
\[
\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} d(c_1a_{11} + \cdots + c_4a_{41}) \\ d(c_1a_{12} + \cdots + c_4a_{42}) \\ d(c_3a_{13} + \cdots + c_4a_{43}) \\ d(c_1a_{14} + \cdots + c_4a_{44}) \end{bmatrix} = dA \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix}
\]
\[
\text{This guarantees that } y_1, \ldots, y_4 \text{ is an integral solution to the quadratic form}
\]
\[
y_1^2 - ay_2^2 - by_3^2 + aby_4^2 = d^2l, \text{ and the relationship between the } y \text{'s and } c \text{'s is as claimed.}
\]

Conversely, if
\[
\begin{bmatrix}
c_1 \\
c_2 \\
c_3 \\
c_4
\end{bmatrix} = \frac{1}{d} A^{-1} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} \in \mathbb{Z}^4,
\]
\[
\text{Then } x = c_1\alpha_1 + \cdots + c_4\alpha_4 \text{ is in } \mathcal{O}. \text{ By the preceding argument, the quadratic form}
\]
on $y$'s is clearly equivalent to $N(x) = l$. 

16
Example 5: We use MAGMA to find the left ideal representatives of $O$ and subsequently a basis for the right order of each representative.

$> A := \text{QuaternionAlgebra}\langle\text{RationalField()}\mid -3,-41\rangle;$
$> O := \text{MaximalOrder}(A);$  
$> \text{[Basis(RightOrder(I)):I in LeftIdealClasses(O)]};$


$$\begin{bmatrix} 1, & 1/2 + 1/2i, & 1/2 + 1/6i + 1/2j + 1/6k, & -1/2 - 1/6i + 1/2j - 1/6k \\ 1/2 + j + 3/2k, & 1/24i + 15/8j + 23/12k, & 2j + k, & 2k \\ 1/2 + 1/2k, & 1/6i + 1/2j + 2/3k, & j, & k \\ 1/2 + j + 1/2k, & 1/12i + 7/4j + 5/6k, & 2j, & k \end{bmatrix}$$

From this result, we have an equation

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \frac{1}{24} \begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 17/12 & 0 & 0 \\ 1 & 2 & 23/12 & 1 \\ 3/2 & 2/12 & 1 & 2 \end{bmatrix}^{-1} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix},$$

where $y_1^2 + 3y_2^2 + 41y_3^2 + 3 \cdot 41y_4^2 = 24^2l$. There are many integer solutions for this equation, but not all satisfy $\frac{1}{d}A^{-1}y \in \mathbb{Z}^4$. For example, $(8,12,2,2)$ is a integral solution where $l = 2$, but $\frac{1}{d}A^{-1}y = (16, 288, -277, -\frac{297}{2})^T \notin \mathbb{Z}^4$. And, $(12,-7,-3,2)$ is another integral solution where $l = 2$, then $\frac{1}{d}A^{-1}y = (1, -7, 6, 3)^T \in \mathbb{Z}^4$. Thus

$$\begin{bmatrix} 1 \\ i \\ j \\ k \end{bmatrix}^T \cdot \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \frac{1}{2} - \frac{7}{24}i - \frac{1}{8}j + \frac{1}{12}k \text{ lies in } O_2 \text{ and has norm 2.}$$
The following table is the elements of small norms in $O_1, O_2, O_3$ and $O_4$.

<table>
<thead>
<tr>
<th>$N(x)$</th>
<th>$O_1$</th>
<th>$O_2$</th>
<th>$O_3$</th>
<th>$O_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\pm 1, \pm \frac{1}{2} \pm \frac{1}{2}i$</td>
<td>$\pm 1$</td>
<td>$\pm 1$</td>
<td>$\pm 1$</td>
</tr>
<tr>
<td>2</td>
<td>none</td>
<td>$\pm (\pm \frac{1}{2} + \frac{2}{3}i - \frac{1}{5}j - \frac{1}{17}k)$</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>3</td>
<td>$\pm i, \pm \frac{2}{2} \pm \frac{1}{2}i$</td>
<td>none</td>
<td>$\pm i$</td>
<td>$\pm (\pm \frac{1}{2} + \frac{1}{7}i + \frac{1}{2}j)$</td>
</tr>
<tr>
<td>5</td>
<td>none</td>
<td>none</td>
<td>$\pm (\pm \frac{1}{2} + \frac{2}{3}i + \frac{1}{6}k)$</td>
<td>$\pm (\pm \frac{3}{2} + \frac{1}{3}i + \frac{1}{4}j)$</td>
</tr>
</tbody>
</table>

4.2 Conclusion Based on Our Computations

From the above table, and recall the table in section 3.3, compare the number of endomorphisms with kernel of degrees 1, 2, 3, 5 and the left ideals of maximal order of norm 1, 2, 3, 5, we have $j = 0$ corresponds to $O_1$, $j = 3$ corresponds to $O_3$, $j = -9$ corresponds to $O_4$, and $j = -13$ corresponds to $O_2$. 
References


This data is the algorithm of $E/C$ where $C$ is a cyclic group with degree 2 by Mathematica ($\alpha = 0$, $p=41$, $j=0$).

\begin{verbatim}
<<Algebra'FiniteFields`
f[x_]:=x^3+x^2+14x
s1[x_]:=( x- GF[41,{3,0,0,0,1}][{20,0,7,0}] ) *( x- GF[41,{3,0,0,0,1}][{20,0,34,0}] )/x
x2Q[x_]:=x^4+GF[41,{3,0,0,0,1}][{13,0,0,0}]*x^2+(GF[41,{3,0,0,0,1}][{32,0,0,0}])
For[i=0,i<41,i++,For[k=0,k<41,k++,If[x2Q[GF[41,{3,0,0,0,1}][{i,0,k,0}]==0,Print[{i,0,k,0}];
];
];]
{0,0,3,0}
{0,0,38,0}
t1:=s1[GF[41,{3,0,0,0,1}][{0,0,3,0}]]
t2:=s1[GF[41,{3,0,0,0,1}][{0,0,38,0}]]
t1
t2
-(t1+t2)
t1*t2
{1, 0, 6, 0}41
{1, 0, 35, 0}41
{39, 0, 0, 0}41
{27, 0, 0, 0}41

a1:=0
a3:=0
a2:=GF[41,{3,0,0,0,1}][{39,0,0,0}]
a4:=GF[41,{3,0,0,0,1}][{27,0,0,0}]
a6:=0
b2:=(a1^2)+4*a2
b4:=2*a4+a1*a3
b6:=a3^2+4*a6
b8:=(a1^2)*a6+4*a2*a6-a1*a3*a4+a2*(a3^2)-a4^2
c4:=b2^2-24*b4
d:=-b2^2*b8-8*b4^3-27*b6^2+9*b2*b4*b6
j:=c4^3/d
j
{3, 0, 0, 0}41
\end{verbatim}
The algorithm of $E/C$ where $C$ is a cyclic group with degree 3

$$x^{P_i} = -14, \ p=41, \ j=0$$

```plaintext
<<Algebra`FiniteFields`

f[x_] := x^3 + x^2 + 14*x

Factor[(x^4 - 2*14*x^2 + 14^2) - 4*(x^3 + x^2 + 14*x)*x, Modulus -> 41]

PolynomialMod[14/-14, 41]
```

40

```plaintext
z[t_] := t*(t-40)^2/(t+14)^2

t1 := z[GF[41, {3, 0, 1}][{20, 7}]]

t2 := z[GF[41, {3, 0, 1}][{20, 34}]]

t1

t2

-(t1 + t2)

t1 * t2

{22, 20}_{41}

{22, 21}_{41}

{38, 0}_{41}

{3, 0}_{41}
```

```plaintext
a1 := 0
a3 := 0
a2 := 38
a4 := 3
a6 := 0

b2 := (a1^2) + 4*a2
b4 := 2*a4 + a1*a3
b6 := a3^2 + 4*a6
b8 := (a1^2)*a6 + 4*a2*a6 - a1*a3*a4 + a2*(a3^2) - a4^2

b4 := 2^2 - 24*b4

d := -b2^2 + b8 - 8*b4^3 - 27*b6^2 + 9*b2*b4*b6

j := c4^3/d

PolynomialMod[j, 41]
```

0
The algorithm of E/C where C is a cyclic group with degree 5

\( (xP_1, xP_2 = 20 + \sqrt{-3}, 29 + 4\sqrt{-3}, p = 41, j = 0) \)

\( a1 := 0 \)
\( a3 := 0 \)
\( a2 := 1 \)
\( a4 := 14 \)
\( a6 := 0 \)

\[ x2Q[x_] := (x^4 - 2a4x^2 - 8a6x - 4a2a6 + a4^2)/(4(x^3 + a2x^2 + a4x + a6)) \]

\[ x2Q[x] \]

\[ 196 - 28x^2 + x^4 \]
\[ 4(14x + x^2 + x^3) \]

\[ x4Q[s_] := x2Q[x2Q[x]] \]
\[ x4Q[s_] \]

\[ 196 - 7(196-28x^2, x^4)^2 \]
\[ 4(14x^2 + x^3)^2 \]
\[ + (196-28x^2, x^4)^4 \]
\[ 256(14x^2 + x^3)^4 \]

\[ 196 - \frac{7(196-28x^2, x^4)^2}{16(14x^2 + x^3)^2} \]
\[ + \frac{(196-28x^2, x^4)^2}{64(14x^2 + x^3)^2} \]

\[ \text{PolynomialMod} \left( \frac{196 - 7(196-28x^2, x^4)^2}{4(14x^2 + x^3)^2} + \frac{(196-28x^2, x^4)^4}{256(14x^2 + x^3)^4} \right), 41 \]

\[ 18 + 13x^2 + 5x^3 + 29x^4 + 2x^5 + 5x^6 + 34x^7 + 18x^8 + 20x^9 + 4x^{10} + 13x^{11} + 12x^{12} + 26x^{13} + 6x^{14} + 18x^{15} \]
\[ 3x + 4x^2 + 28x^3 + 12x^4 + 36x^5 + 30x^6 + 10x^7 + 3x^8 + 30x^9 + 24x^{10} + 29x^{11} + 29x^{12} + 39x^{13} + 5x^{14} + x^{15} \]

\[ \text{Factor} \left( 18 + 13x^2 + 5x^3 + 29x^4 + 2x^5 + 5x^6 + 34x^7 + 18x^8 + 20x^9 + 4x^{10} + 13x^{11} + 12x^{12} + 26x^{13} + 6x^{14} + 18x^{16} \right) \]
\[ \times (3x + 4x^2 + 28x^3 + 12x^4 + 36x^5 + 30x^6 + 10x^7 + 3x^8 + 30x^9 + 24x^{10} + 29x^{11} + 29x^{12} + 39x^{13} + 5x^{14} + x^{15}), \text{Modulus} \rightarrow 41 \]

\[ 17 (14 + x) (33 + x) (34 + x + x^2) (4 + 9x + x^2) (6 + 12x + x^2) (34 + 14x + x^2) (35 + 17x + x^2) (26 + 18x + x^2) (28 + 24x + x^2) \]
<<\text{Algebra\textbackslash FiniteFields}\nSolve\{a+c==-1 && \text{Modulus}\rightarrow 41, b+d==0 && \text{Modulus}\rightarrow 41, a^*c-3b^*d==34 && \text{Modulus}\rightarrow 41, a^*d+b^*c==0 && \text{Modulus}\rightarrow 41\},\{a,b,c,d\},\text{Mode}\rightarrow \text{Modular}\nSolve\{a+c==-9 && \text{Modulus}\rightarrow 41, b+d==0 && \text{Modulus}\rightarrow 41, a^*c-3b^*d==4 && \text{Modulus}\rightarrow 41, a^*d+b^*c==0 && \text{Modulus}\rightarrow 41\},\{a,b,c,d\},\text{Mode}\rightarrow \text{Modular}\nSolve\{a+c==-12 && \text{Modulus}\rightarrow 41, b+d==0 && \text{Modulus}\rightarrow 41, a^*c-3b^*d==6 && \text{Modulus}\rightarrow 41, a^*d+b^*c==0 && \text{Modulus}\rightarrow 41\},\{a,b,c,d\},\text{Mode}\rightarrow \text{Modular}\nSolve\{a+c==-14 && \text{Modulus}\rightarrow 41, b+d==0 && \text{Modulus}\rightarrow 41, a^*c-3b^*d==34 && \text{Modulus}\rightarrow 41, a^*d+b^*c==0 && \text{Modulus}\rightarrow 41\},\{a,b,c,d\},\text{Mode}\rightarrow \text{Modular}\nSolve\{a+c==-17 && \text{Modulus}\rightarrow 41, b+d==0 && \text{Modulus}\rightarrow 41, a^*c-3b^*d==35 && \text{Modulus}\rightarrow 41, a^*d+b^*c==0 && \text{Modulus}\rightarrow 41\},\{a,b,c,d\},\text{Mode}\rightarrow \text{Modular}\nSolve\{a+c==-18 && \text{Modulus}\rightarrow 41, b+d==0 && \text{Modulus}\rightarrow 41, a^*c-3b^*d==26 && \text{Modulus}\rightarrow 41, a^*d+b^*c==0 && \text{Modulus}\rightarrow 41\},\{a,b,c,d\},\text{Mode}\rightarrow \text{Modular}\nSolve\{a+c==-24 && \text{Modulus}\rightarrow 41, b+d==0 && \text{Modulus}\rightarrow 41, a^*c-3b^*d==28 && \text{Modulus}\rightarrow 41, a^*d+b^*c==0 && \text{Modulus}\rightarrow 41\},\{a,b,c,d\},\text{Mode}\rightarrow \text{Modular}\n\{(\text{Modulus}\rightarrow 41, a\rightarrow 16, b\rightarrow 11, c\rightarrow 16, d\rightarrow 30), (\text{Modulus}\rightarrow 41, a\rightarrow 16, b\rightarrow 30, c\rightarrow 15, d\rightarrow 11)\}\n\{(\text{Modulus}\rightarrow 41, a\rightarrow 15, b\rightarrow 11, c\rightarrow 16, d\rightarrow 30), (\text{Modulus}\rightarrow 41, a\rightarrow 16, b\rightarrow 30, c\rightarrow 15, d\rightarrow 11)\}\n\{(\text{Modulus}\rightarrow 41, a\rightarrow 35, b\rightarrow 20, c\rightarrow 35, d\rightarrow 21), (\text{Modulus}\rightarrow 41, a\rightarrow 35, b\rightarrow 21, c\rightarrow 35, d\rightarrow 20)\}\n\{(\text{Modulus}\rightarrow 41, a\rightarrow 34, b\rightarrow 6, c\rightarrow 34, d\rightarrow 35), (\text{Modulus}\rightarrow 41, a\rightarrow 34, b\rightarrow 35, c\rightarrow 34, d\rightarrow 6)\}\n\{(\text{Modulus}\rightarrow 41, a\rightarrow 12, b\rightarrow 14, c\rightarrow 12, d\rightarrow 27), (\text{Modulus}\rightarrow 41, a\rightarrow 12, b\rightarrow 27, c\rightarrow 12, d\rightarrow 14)\}\n\{(\text{Modulus}\rightarrow 41, a\rightarrow 32, b\rightarrow 3, c\rightarrow 32, d\rightarrow 3), (\text{Modulus}\rightarrow 41, a\rightarrow 32, b\rightarrow 38, c\rightarrow 32, d\rightarrow 3)\}\n\{(\text{Modulus}\rightarrow 41, a\rightarrow 29, b\rightarrow 4, c\rightarrow 29, d\rightarrow 37), (\text{Modulus}\rightarrow 41, a\rightarrow 29, b\rightarrow 37, c\rightarrow 29, d\rightarrow 4)\}\n8 < 41
8 < 41
8 < 41
8 < 41
\text{xt0}[\text{GF}[41,\{3,0,1\}][{20,1}]]
(29, 4)_{41}
\text{GF}[41,\{3,0,1\}][{14}] / \text{GF}[41,\{3,0,1\}][{20,1}]
\text{GF}[41,\{3,0,1\}][{14}] / \text{GF}[41,\{3,0,1\}][{29,4}]
(1, 2)_{41}
(35, 39)_{41}
f[t_]:=(t-\text{GF}[41,\{3,0,1\}][{1,2}])^2(\text{GF}[41,\{3,0,1\}][{35,39}])^2(\text{GF}[41,\{3,0,1\}][{20,1}])^2(\text{GF}[41,\{3,0,1\}][{29,4}])^2
\text{t1:=f[GF}[41,\{3,0,1\}][{20,7}]]
\text{t2:=f[GF}[41,\{3,0,1\}][{20,34}]]
\text{t1}
\text{t2}
(3, 19)_{41}
(33, 11)_{41}
\[ z(t) = t(t-GF[41,\{3,0,1\}][\{3,19\}])*(t-GF[41,\{3,0,1\}][\{33,11\}]) \]

\text{Coefficient}[z(t), t^2] \\
\text{Coefficient}[z(t), t] \\
\{5, 11\}_{41} \\
\{5, 4\}_{41} \\
\text{a1} := 0 \\
\text{a3} := 0 \\
\text{a2} := GF[41,\{3,0,1\}][\{5,11\}] \\
\text{a4} := GF[41,\{3,0,1\}][\{5,4\}] \\
\text{a6} := 0 \\
\text{b2} := (\text{a1}^2) + 4*\text{a2} \\
\text{b4} := 2*\text{a4} + \text{a1} * \text{a3} \\
\text{b6} := \text{a3}^2 + 4*\text{a6} \\
\text{b8} := (\text{a1}^2) * \text{a6} + 4*\text{a2} * \text{a6} - \text{a1} * \text{a3} * \text{a4} + \text{a2} * (\text{a3}^2) - \text{a4}^2 \\
\text{c4} := \text{b2}^2 - 24*\text{b4} \\
\text{d} := -\text{b2}^2 * \text{b8} - 8*\text{b4}^3 - 27*\text{b6}^2 + 9*\text{b2} * \text{b4} * \text{b6} \\
\text{j} := \text{c4}^3 / \text{d} \\
\text{j} \\
\{28, 0\}_{41}