A New Algorithm for Computing Endomorphism Rings of Supersingular Elliptic Curves

Ken McMurdy
Ramapo College of New Jersey

January 10, 2013
Supersingular Elliptic Curves

**Definition:** Fix a prime $p > 2$. Then an elliptic curve $E$ over $\overline{\mathbb{F}}_p$ is a smooth curve given by an equation of the form

$$y^2 = x^3 + ax^2 + bx + c \quad a, b, c \in \overline{\mathbb{F}}_p.$$ 

**Key Fact:** The points of $E$ form an abelian group, with the infinite point serving as the identity.

**Definition:** We say that $E$ is ordinary if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ and supersingular if $E[p]$ is trivial.

---

Ken McMurdy Ramapo College of New Jersey

A New Algorithm for Computing Endomorphism Rings of Supersingular Elliptic Curves
**Definition:** Fix a prime $p > 2$. Then an elliptic curve $E$ over $\overline{F}_p$ is a smooth curve given by an equation of the form

$$y^2 = x^3 + ax^2 + bx + c \quad a, b, c \in \overline{F}_p.$$

**Key Fact:** The points of $E$ form an abelian group, with the infinite point serving as the identity.

**Definition:** We say that $E$ is ordinary if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ and supersingular if $E[p]$ is trivial.

**Theorem:** There are $\left\lfloor \frac{p}{12} \right\rfloor + \epsilon$ supersingular elliptic curves over $\overline{F}_p$, where $\epsilon = 0, 1, 1,$ or $2$, when $p \equiv 1, 5, 7,$ or $11 \pmod{12}$. They are all defined over $\mathbb{F}_{p^2}$ and there is a simple formula.

**Example:** When $p = 79$, there are seven s.s. elliptic curves.

$$j = 15, 17, 21, 64, 69 (1728); \quad j^2 + 14j + 62 = 0$$
Theorem: Let $\mathbb{Q}_p,\infty$ be the unique quaternion algebra over $\mathbb{Q}$ which is ramified only at $p$ and $\infty$. Let $A/F_p$ be a supersingular elliptic curve. Then there is an isomorphism

$$\iota_A : \mathbb{Q}_p,\infty \sim \text{End} A \otimes \mathbb{Q}.$$
Deuring’s Theorem

**Theorem:** Let $\mathbb{Q}_{p,\infty}$ be the unique quaternion algebra over $\mathbb{Q}$ which is ramified only at $p$ and $\infty$. Let $A/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve. Then there is an isomorphism

$$\iota_A : \mathbb{Q}_{p,\infty} \xrightarrow{\sim} \text{End } A \otimes \mathbb{Q}.$$ 

1. $R := \iota_A^{-1}(\text{End } A)$ is a maximal order in $\mathbb{Q}_{p,\infty}$. 
2. For any $\phi \in \text{End } A$, $N(\iota_A^{-1}\phi) = \deg \phi$. 
3. The correspondence between maximal orders and s.s. elliptic curves is basically one-to-one.
Deuring’s Theorem

**Theorem:** Let $\mathbb{Q}_{p,\infty}$ be the unique quaternion algebra over $\mathbb{Q}$ which is ramified only at $p$ and $\infty$. Let $A/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve. Then there is an isomorphism

$$\iota_A : \mathbb{Q}_{p,\infty} \xrightarrow{\sim} \text{End} A \otimes \mathbb{Q}.$$ 

(1) $R := \iota_A^{-1}(\text{End} A)$ is a maximal order in $\mathbb{Q}_{p,\infty}$.

(2) For any $\phi \in \text{End} A$, $N(\iota_A^{-1} \phi) = \deg \phi$.

(3) The correspondence between maximal orders and s.s. elliptic curves is basically one-to-one.

**Problem:** How do we most efficiently match curves with orders, and explicitly represent the corresponding isomorphisms?
Theorem: (Pizer) Let \( \mathfrak{A}(m, n) = \{a + bi + cj + dk | a, b, c, d \in \mathbb{Q}\} \), where \( i^2 = m, j^2 = n, \) and \( ij = k = -ji \). Then

\[
\mathbb{Q}_{p, \infty} \cong \begin{cases} 
\mathfrak{A}(-1, -p), & \text{if } p \equiv 3 \pmod{4} \\
\mathfrak{A}(-2, -p), & \text{if } p \equiv 5 \pmod{8} \\
\mathfrak{A}(-p, -q), & \text{if } p \equiv 1 \pmod{8},
\end{cases}
\]

where \( q \) is prime, \( q \equiv 3 \pmod{4} \), and \( \left(\frac{p}{q}\right) = -1 \).
Explicit Representation of $\mathbb{Q}_p,\infty$

**Theorem:** (Pizer) Let $\mathfrak{A}(m, n) = \{a + bi + cj + dk | a, b, c, d \in \mathbb{Q}\}$, where $i^2 = m$, $j^2 = n$, and $ij = k = -ji$. Then

$$
\mathbb{Q}_p,\infty \cong \begin{cases} 
\mathfrak{A}(-1, -p), & \text{if } p \equiv 3 \pmod{4} \\
\mathfrak{A}(-2, -p), & \text{if } p \equiv 5 \pmod{8} \\
\mathfrak{A}(-p, -q), & \text{if } p \equiv 1 \pmod{8},
\end{cases}
$$

where $q$ is prime, $q \equiv 3 \pmod{4}$, and $\left(\frac{p}{q}\right) = -1$.

**Theorem:** (Pizer) Representing $\mathbb{Q}_p,\infty$ as above (in each case), a $\mathbb{Z}$-basis for one particular maximal order is given by:

$$
\begin{align*}
\frac{1}{2}(1 + j), & \frac{1}{2}(i + k), j, k & \text{if } p \equiv 3 \pmod{4} \\
\frac{1}{2}(1 + j + k), & \frac{1}{4}(i + 2j + k), j, k & \text{if } p \equiv 5 \pmod{8} \\
\frac{1}{2}(1 + j), & \frac{1}{2}(i + k), \frac{1}{q}(j + rk), k & \text{if } p \equiv 1 \pmod{8},
\end{align*}
$$

where $r \in \mathbb{Z}$ such that $q \mid (r^2p + 1)$. 
Fix a supersingular elliptic curve $A/\mathbb{F}_{p^2}$. Recall that there exists

$$\iota_A : \mathbb{Q}_{p, \infty} \sim \text{End } A \otimes \mathbb{Q}.$$ 

Let $R = \iota_A^{-1}(\text{End } A)$. Then $R$ is a maximal order in $\mathbb{Q}_{p, \infty}$.

**Theorem:** Suppose $\phi : A \rightarrow B$ is an isogeny of degree $n$. Let $\psi : B \rightarrow A$ be the dual isogeny. Then there is an isomorphism,

$$\iota_B : \mathbb{Q}_{p, \infty} \sim \text{End } B \otimes \mathbb{Q},$$

given by

$$\iota_B(\alpha) = \frac{1}{n} \phi \circ \iota_A(\alpha) \circ \psi.$$
Fix a supersingular elliptic curve $A/\mathbb{F}_{p^2}$. Recall that there exists

$$\iota_A : \mathbb{Q}_p,\infty \rightarrow \text{End } A \otimes \mathbb{Q}.$$ 

Let $R = \iota_A^{-1}(\text{End } A)$. Then $R$ is a maximal order in $\mathbb{Q}_p,\infty$.

**Theorem:** Suppose $\phi : A \rightarrow B$ is an isogeny of degree $n$. Let $\psi : B \rightarrow A$ be the dual isogeny. Then there is an isomorphism,

$$\iota_B : \mathbb{Q}_p,\infty \rightarrow \text{End } B \otimes \mathbb{Q},$$

given by

$$\iota_B(\alpha) = \frac{1}{n} \phi \circ \iota_A(\alpha) \circ \psi.$$

**Main Strategy:** Match one endomorphism ring explicitly. Then systematically generate all others by applying isogenies.
Definition: (1) If $H \subseteq A$ is a finite subgroup, let

$$I_H = \{ \tau \in \text{End } A \mid H \subseteq \text{Ker}(\tau) \}.$$ 

Then $I_H$ is clearly a left ideal of $\text{End } A$.

(2) Conversely, suppose $I \subseteq \text{End } A$ is a left ideal. Let

$$H(I) = \bigcap_{\tau \in I} \text{Ker}(\tau).$$

Then $H(I)$ is a subgroup of $A$ (finite if $I \neq 0$).

(3) We say that $I$ is a kernel ideal if $I = I_{H(I)}$. 
Kernel Ideals

**Definition:** (1) If $H \subseteq A$ is a finite subgroup, let

$$I_H = \{ \tau \in \text{End } A \mid H \subseteq \text{Ker}(\tau) \}.$$ 

Then $I_H$ is clearly a left ideal of $\text{End } A$.

(2) Conversely, suppose $I \subseteq \text{End } A$ is a left ideal. Let

$$H(I) = \bigcap_{\tau \in I} \text{Ker}(\tau).$$

Then $H(I)$ is a subgroup of $A$ (finite if $I \neq 0$).

(3) We say that $I$ is a *kernel ideal* if $I = I_{H(I)}$.

**Theorem:** For a supersingular $A$, every left ideal is a kernel ideal!

**Theorem:** Suppose $I \subseteq \text{End } A$ is a left ideal. Let $B = A/H(I)$, and let $\phi : A \rightarrow B$ be the canonical isogeny. Then $\nu_B^{-1}(\text{End } B)$ contains the right order of $I$. If $I$ is a kernel ideal, they are equal.
The Algorithm

Suppose \( \nu_A \) is explicit, and \( R = \nu_A^{-1}(\text{End } A) \) is explicit. Let \( P \in A \) be a point of order 2. Let \( B = A/\langle P \rangle \). Then we can obtain \( R' = \nu_B^{-1}(\text{End } B) \) explicitly, and then \( \nu_B \) explicitly (on a \( \mathbb{Z} \)-basis for \( R' \)), with the following steps.

1. Compute \( I = I_{\langle P \rangle} \) (a calculation in \( R/2R \), via \( \nu_A \)).
2. Compute \( R' = \) the right order of \( I \) (a calculation in \( \mathbb{Q}_p, \infty \)).
   By above, we know that \( R' = \nu_B^{-1}(\text{End } B) \).
3. Use \( \nu_B(\alpha) = \frac{1}{2} \phi \circ \nu_A(\alpha) \circ \psi \) to compute \( \nu_B \) on a \( \mathbb{Z} \)-basis for \( R' \).
The Algorithm

Suppose $\iota_A$ is explicit, and $R = \iota_A^{-1}(\text{End } A)$ is explicit. Let $P \in A$ be a point of order 2. Let $B = A/\langle P \rangle$. Then we can obtain $R' = \iota_B^{-1}(\text{End } B)$ explicitly, and then $\iota_B$ explicitly (on a $\mathbb{Z}$-basis for $R'$), with the following steps.

1. Compute $I = I_{\langle P \rangle}$ (a calculation in $R/2R$, via $\iota_A$).
2. Compute $R' = \text{the right order of } I$ (a calculation in $\mathbb{Q}_p, \infty$).
   By above, we know that $R' = \iota_B^{-1}(\text{End } B)$.
3. Use $\iota_B(\alpha) = \frac{1}{2} \phi \circ \iota_A(\alpha) \circ \psi$ to compute $\iota_B$
on a $\mathbb{Z}$-basis for $R'$.

Theorem: (Ribet) Any two supersingular elliptic curves are 2-power isogenous.

So by doing this $O(p)$ times, we obtain explicit representations of $\text{End } A$ for each supersingular elliptic curve $A$. 

Ken McMurdy Ramapo College of New Jersey

A New Algorithm for Computing Endomorphism Rings of Supersingular Elliptic Curves
Example of the Isogeny Mechanism

Step 1: Start with $y^2 = x^3 - x$. So $j(A) = 69 \equiv 1728$.

Step 2: Determine $\iota_A$ explicitly on $R = \iota_A^{-1}(\text{End } A)$.
(This is easy, since $j = 1728$ is such a special curve!)

$$
\iota_A(i) = (-x, iy) \quad \text{where } i^2 = -1 \text{ in } \mathbb{F}_{p^2}
$$

$$
\iota_A(j) = (x^{79}, y^{79})
$$

$$
= (x^{79}, (x^{117} + 40x^{115} + \cdots + 39x^{41} + 78x^{39})y)
$$

$$
\iota_A(k) = \iota_A(i) \circ \iota_A(j)
$$

$$
\iota_A(\frac{1}{2} + \frac{1}{2}j) = \left( \frac{36x^{20} + 45x^{19} + \cdots + 73x + 4}{9x^{19} + 31x^{18} + \cdots + 75x + 4}, \frac{21x^{29} + 40x^{28} + \cdots + 12x + 71}{52x^{29} + 5x^{28} + \cdots + 71x + 8}y \right)
$$

$$
\iota_A(\frac{1}{2}i + \frac{1}{2}k) = \iota_A(i) \circ \iota_A(\frac{1}{2} + \frac{1}{2}j)
$$
Step 3: Compute the images of the three degree 2 isogenies.

\( P = (0, 0) \) \[ \left( \frac{x^2 - 1}{x}, \frac{x^2 + 1}{x^2} y \right) \quad y^2 = x^3 + 4x \quad j = 69 \]

\( P = (-1, 0) \) \[ \left( \frac{x^2 - x}{x + 1}, \frac{x^2 + 2x - 1}{(x + 1)^2} y \right) \quad y^2 = x^3 + 6x^2 + x \quad j = 15 \]

\( P = (1, 0) \) \[ \left( \frac{x^2 + x}{x - 1}, \frac{x^2 - 2x - 1}{(x - 1)^2} y \right) \quad y^2 = x^3 + 73x^2 + x \quad j = 15 \]

Step 4: Determine the Left (Kernel) Ideal \( I = I(\langle(-1, 0)\rangle) \).

\[ I = \mathbb{Z} \left[ \frac{1}{2} + \frac{1}{2} j, \frac{1}{2} i + \frac{1}{2} k, 2j, 2k \right] \]

Step 5: Determine the Right Order of \( I \).

\[ R' = \iota^{-1}_B(\text{End } B) = \mathbb{Z} \left[ \frac{1}{2} + \frac{1}{2} j, \frac{1}{4} i + \frac{1}{4} k, j, 2i \right] \]
Step 6: Apply $\iota_B(\alpha) = \frac{1}{2} \phi \circ \iota_A(\alpha) \circ \psi$ to basis for $R'$.

\[
\frac{1}{2} + \frac{1}{2}j \rightarrow \left( \frac{4x^{20} + 10x^{19} + \cdots + x^2 + x}{x^{19} + x^{18} + \cdots + 10x + 4}, \frac{73x^{29} + 7x^{28} + \cdots + 5x + 49}{19x^{29} + 70x^{28} + \cdots + 67x + 19} \right)
\]

\[
\frac{1}{4} i + \frac{1}{4} k \rightarrow \left( \frac{63x^5 + 67x^4 + 7x^3 + 56x^2 + 45x + 53}{x^4 + 48x^3 + 63x^2 + 12x + 5}, \frac{10ix^6 + 9ix^5 + 51ix^4 + 12ix^3 + 49ix^2 + 40i}{52x^6 + 31x^5 + 72x^4 + 3x^3 + 18x^2 + 76x + 65} \right)
\]

\[
j \rightarrow (x^{79}, y^{79})
\]

\[
2i \rightarrow \left( \frac{5x^4 + 40x^3 + 70x^2 + 40x + 5}{59x^3 + 40x^2 + 59x}, \frac{50ix^5 + 8ix^4 + ix^3 + ix^2 + 8ix + 50i}{5x^5 + 64x^4 + 15x^3 + 74x^2} \right)
\]
2-isogeny Tree for $p = 79$

\[ j = 69 = 1728 \]

\[ 69 \quad 15 \quad 15 \]

\[ 21 \quad 69 \quad 64 \]

\[ 15 \quad 17 \quad 21 \quad 15 \]

\[ j^2 + 14j + 62 \]