Computing the endomorphism ring of an ordinary elliptic curve

Andrew V. Sutherland
Massachusetts Institute of Technology

April 3, 2009

joint work with Gaetan Bisson

http://arxiv.org/abs/0902.4670
Elliptic curves

An elliptic curve $E/F$ is a smooth projective curve of genus 1 with a distinguished rational point $0$.

The set $E(F)$ of rational points on $E$ form an abelian group.

For $\text{char}(F) \neq 2, 3$ we define $E$ with an affine equation

$$y^2 = x^3 + Ax + B,$$

where $4A^3 + 27B^2 \neq 0$. The $j$-invariant of $E$ is

$$j(E) = 12^3 \frac{4A^3}{4A^3 + 27B^2}.$$

If $F = \overline{F}$ then $j(E)$ uniquely identifies $E$ (but not in $\mathbb{F}_q$).
Elliptic curves over finite fields

Consider $F = \mathbb{F}_q$. The size of the group $E(\mathbb{F}_q)$ is

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

for some integer $t$ with $|t| \leq 2\sqrt{q}$. The SEA algorithm computes $t$ in polynomial time (very fast in practice).

Typically $t$ is nonzero in $\mathbb{F}_q$, in which case $E$ is called ordinary.

Some useful facts about $t = t(E)$:

1. $t(E_1) = t(E_2) \iff E_1$ and $E_2$ are isogenous.
2. $j(E_1) = j(E_2)$ and $t(E_1) = t(E_2) \iff E_2 \cong E_2$.
3. $j(E_1) = j(E_2) \implies |t(E_1)| = |t(E_2)|$ for $j(E_1) \notin \{0, 12^3\}$. 
Maps between elliptic curves

An *isogeny* \( \phi : E_1 \rightarrow E_2 \) is a rational map (defined over \( \overline{F} \)) with \( \phi(0) = 0 \). It induces a homomorphism from \( E_1(F) \) to \( E_2(F) \).

The *endomorphism ring* \( \text{End}(E) \) contains all \( \phi : E \rightarrow E \). We have \( \mathbb{Z} \subseteq \text{End} E \), but for \( F = \mathbb{F}_q \), equality never holds.

If \( E/\mathbb{F}_q \) is ordinary, then \( \text{End}(E) \cong \mathcal{O}(D) \) where

\[
\mathcal{O}(D) = \mathbb{Z} + \frac{D + \sqrt{D}}{2} \mathbb{Z}
\]

is the imaginary quadratic order of some discriminant \( D \).

We want to compute \( D \).
The Frobenius endomorphism

The endomorphism \( \pi : (x, y) \mapsto (x^q, y^q) \) on \( E(\overline{\mathbb{F}_q}) \) satisfies

\[ \pi^2 - t\pi + q = 0. \]

If we set \( D_\pi = t^2 - 4q \) and fix an isomorphism \( \text{End} E \cong \mathcal{O}(D) \) we may regard \( \pi = \frac{t+\sqrt{D_\pi}}{2} \) as an element of \( \mathcal{O}(D) \).

Thus \( \mathcal{O}(D_\pi) \subseteq \mathcal{O}(D) \), which implies \( D|D_\pi \) and that \( D \) and \( D_\pi \) have the same fundamental discriminant \( D_K \).

By factoring \( D_\pi = \nu^2 D_K \) we may determine \( D_K \) and \( \nu \).

We then have \( D = u^2 D_K \) for some \( u|\nu \).

We want to compute \( u \).

This is easy if \( \nu \) is small (or smooth), but may be hard if not.
Computing isogenies

We call a (separable) isogeny \( \phi \) an \( \ell \)-isogeny if \( \# \ker \phi = \ell \). We restrict to prime \( \ell \), in which case \( \ker \phi \) is cyclic.

The classical modular polynomial \( \Phi_\ell \in \mathbb{Z}[X, Y] \) has the property

\[
\Phi_\ell(j(E_1), j(E_2)) = 0 \iff E_1 \text{ and } E_2 \text{ are } \ell\text{-isogenous}.
\]

The \( \ell \)-isogeny graph \( G_\ell(\mathbb{F}_q) \) has vertex set

\[
\mathcal{E}(\mathbb{F}_q) = \{ j(E/\mathbb{F}_q) \} = \mathbb{F}_q,
\]

and edges \((j_1, j_2)\) for \( \Phi_\ell(j_1, j_2) = 0 \) (note \( \Phi_\ell \) is symmetric).

\( \Phi_\ell \) is big: \( O(\ell^{3+\epsilon}) \) bits.
The structure of the $\ell$-isogeny graph [Kohel]

The connected components of $G_\ell(\mathbb{F}_q)$ are $\ell$-volcanoes. An $\ell$-volcano of height $h$ has vertices in level $V_0, \ldots, V_h$.

Vertices in $V_0$ have endomorphism ring $\mathcal{O}(D_0)$ with $\ell \nmid u_0$. Vertices in $V_k$ have endomorphism ring $\mathcal{O}(\ell^{2k}D_0)$.

1. The subgraph on $V_0$ is a cycle (the surface).
   All other edges lie between $V_k$ and $V_{k+1}$ for some $k$.
2. For $k > 0$ each vertex in $V_k$ has one neighbor in $V_{k-1}$.
3. For $k < h$ every vertex in $V_k$ has degree $\ell + 1$.

See [Kohel 1996], [Fouquet-Morain 2002], or [S 2009] for more details.
A 3-volcano of height 2 with a 4-cycle
Algorithms to compute $u$

- **Isogeny climbing**: computes $\ell$-isogenies for prime $\ell|\nu$ to determine the power of $\ell$ dividing $u$ in. Probabilistic complexity $O(q^{3/2+\epsilon})$.

- **Kohel’s algorithm**: computes the kernel of $n$-isogenies, where $n = O(q^{1/6})$ need not be a divisor of $\nu$. Deterministic complexity $O(q^{1/3+\epsilon})$ (GRH).

- **New algorithm**: computes the cardinality of smooth relations using isogenies of subexponential degree. Probabilistic complexity $L[1/2, \sqrt{3}/2](q)$ (GRH+).

\[
L[\alpha, c](x) = \exp \left( (c + o(1)) (\log x)^\alpha (\log \log x)^{1-\alpha} \right).
\]

All algorithms have unconditionally correct output.
The action of the class group [CM theory]

For an invertible ideal \( a \subset \mathcal{O}_D \cong \text{End}(E) \), let \( E[a] \) be the subgroup of points annihilated by all \( a \in a \). The map

\[
j(E) \to j(E/E[a])
\]
corresponds to an isogeny of degree \( N(a) \).

This defines a group action by the ideal group on the set

\[
\{j(E/\mathbb{F}_q) : \text{End}(E) \cong \mathcal{O}(D)\}.
\]

This action factors through the class group \( \text{cl}(\mathcal{O}(D)) = \text{cl}(D) \). The action is faithful and transitive.

See the books of [Cox], [Lang], or [Silverman] for more on CM theory.
If $\ell \nmid v$ and $\left( \frac{D}{\ell} \right) = 1$, the $\ell$-volcano containing $j(E)$ is a cycle of length $|\alpha|$, where $\alpha \in \text{cl}(D)$ contains an ideal of norm $\ell$.

We can compute $|\alpha|$ (without knowing $D$) by walking a path $j_0, j_1, \ldots$ in $G_\ell(\mathbb{F}_q)$ starting from $j_0 = j(E)$:

1. Let $j_1$ be one of the two roots of $\Phi_\ell(X, j_0)$ in $\mathbb{F}_q$.
2. Let $j_{k+1}$ be the unique root of $\Phi_\ell(X, j_k) / (X - j_{k-1})$ in $\mathbb{F}_q$.

The choice of $j_1$ is arbitrary (we cannot distinguish $\alpha$ and $\alpha^{-1}$). In either case, $|\alpha|$ (and $|\alpha^{-1}|$) is the least $n$ for which $j_n = j_0$.

Step 2 finds the unique root of a degree $\ell$ polynomial $f(X)$ over $\mathbb{F}_q$. Complexity is $T(\ell) = O(\ell^2 + M(\ell) \log q)$ operations in $\mathbb{F}_q$. 

Andrew V. Sutherland  
Computing the endomorphism ring of an ordinary elliptic curve
Computing \( \text{End}(E) \) with class groups (naïvely)

Given \( E/\mathbb{F}_q \), let \( \#E = q + 1 - t \) and \( 4q = t^2 - v^2 D_K \), so that \( \text{End}(E) \cong \mathcal{O}(D) \) where \( D = u^2 D_K \) for some \( u \mid v \).

If \( u_1, \ldots, u_m \) are the divisors of \( v \), then \( u = u_i \) for some \( i \).

Pick any \( \ell \nmid v \) satisfying \( \left( \frac{D_K}{\ell} \right) = 1 \).

For each \( D_i = u_i^2 D_K \) there is an element \( \alpha_i \in \text{cl}(D_i) \) containing an ideal of norm \( \ell \), but \( \vert \alpha_i \vert \) typically varies with \( i \).

We can compare \( \vert \alpha_i \vert \) to the length of the \( \ell \)-isogeny cycle containing \( j(E) \). These must be equal if \( u = u_i \).

This is too slow, but we can exploit this idea.
Relations

A relation $R$ is a pair of vectors $(\ell_1, \ldots, \ell_k)$ and $(e_1, \ldots, e_k)$.

We say $R$ holds in $\text{cl}(D)$ if for each $i$ there is an $\alpha_i \in \text{cl}(D)$ containing an ideal of norm $\ell_i$ such that

$$\alpha_1^{e_1} \cdots \alpha_k^{e_k} = 1.$$ 

More generally, we define the cardinality of $R$ in $\text{cl}(D)$ by

$$\# R / D = \# \left\{ \tau \in \{\pm 1\}^k : \prod \alpha_i^{\tau_i e_i} = 1 \text{ in } \text{cl}(D) \right\}.$$ 

$\# R / D$ does not depend on the choice of $\alpha_i$. 

Andrew V. Sutherland

Computing the endomorphism ring of an ordinary elliptic curve
Counting relations

Given a relation $R$ with $(\ell_1, \ldots, \ell_k)$ and $(e_1, \ldots, e_k)$:

1. Set $J_0$ be a list containing the single element $j(E)$.
2. For each element in $J_i$ walk $e_i$ steps in both directions of the $\ell_i$ cycle and append the two end points to the list $J_{i+1}$.
3. $\#R/E$ is the number of times $j(E)$ appears in the list $J_k$.

The complexity is $\sum_{i=1}^k 2^i e_i T(\ell_i)$ operations in $\mathbb{F}_q$. 
The key lemma

**Lemma:** If $\mathcal{O}(D_1) \subseteq \mathcal{O}(D_2)$ then $\#R/D_1 \leq \#R/D_2$.

**Proof:** There is a norm-preserving map from $\mathcal{O}(D_1)$ to $\mathcal{O}(D_2)$ that induces a group homomorphism from $\text{cl}(D_1)$ to $\text{cl}(D_2)$.

**Corollary:** Let $p \parallel v$ and set $D_1 = (v/p)^2 D_K$ and $D_2 = p^2 D_K$. Let $R$ be a relation with $\#R/D_1 > \#R/D_2$. If $u$ is the conductor of $\mathcal{O}(D) \cong \text{End}(E)$ then

$$p | u \iff \#R/E < \#R/D_1.$$

**Theorem:** Such an $R$ exists.

**Conjecture:** Almost all $R$ that hold in $\text{cl}(D_1)$ don’t hold in $\text{cl}(D_2)$. 

Andrew V. Sutherland

Computing the endomorphism ring of an ordinary elliptic curve
Algorithm to compute $\text{End}(E)$

Given $E/\mathbb{F}_q$, the following algorithm computes $D = u^2 D_K$, the discriminant of the order isomorphic to $\text{End}(E)$.

1. Compute $t = q + 1 - \#E$, $v$, and $D_k$, with $4q = t^2 - v^2 D_K$.
2. For primes $p | v$, find a relation $R$ satisfying the corollary. Count $\#R/E$ in the isogeny graph to test whether $p | u$.
3. Output $u^2 D_K$.

The algorithm above assumes $v$ is square-free.
Finding smooth relations

The following algorithm is adapted from Hafner/McCurley.

We seek a smooth relation in $\text{cl}(D_1)$.

Pick a smoothness bound $B$ and a small constant $k_0$ (say 3).

1. Let $\ell_1, \ldots, \ell_n$ be the primes up to $B$ with $\left(\frac{D_1}{\ell_i}\right) = 1$, and let $\alpha_i \in \text{cl}(D_1)$ contain an ideal of norm $\ell_i$.

2. Generate $\beta = \prod \alpha_i^{x_i}$ where all but $k_0$ of the $x_i$ are zero and the other $x_i$ are suitably bounded.

3. For each $\beta$, test whether $N(b)$ is $B$-smooth, where $b$ is the reduced representative of $\beta$.

4. If so write $\prod \alpha_i^{x_i} = \prod \alpha_i^{y_i}$ and compute $R$. Verify that $\#R/D_1 > \#R/D_2$ (almost always true).

For suitable $B$, the complexity is $L[1/2, \sqrt{3}/2](|D|)$
An example of cryptographic size (200 bits)

We have $4q = t^2 - v^2 D_K$ where $t = 212$, $D_K = -7$ and

$$v = 2 \cdot 127 \cdot \underbrace{524287}_{p_1} \cdot \underbrace{71957776666870732918103}_{p_2}.$$

After finding $2 \nmid u$ and $127 \nmid u$ we test $p_1 | u$ by computing

$$R_1 = (2^{2533}, 11^{752}, 29^2, 37^47, 79^1, 113^1, 149^1, 151^2, 347^1, 431^1),$$

which holds in $\text{cl}(p_2^2 D_K)$ but not $\text{cl}(p_1^2 D_K)$. We test $p_2 | u$ using

$$R_2 = (2^{23}, 11^5, 43^1, 71^2),$$

which holds in $\text{cl}(p_1^2 D_K)$ but not in $\text{cl}(p_2^2 D_K)$.

Total time to compute $\text{End}(E)$ is under 30 minutes.
Certifying the endomorphism ring

To verify a claimed value of \( u \), it suffices to have a relation \( R_p \) for each prime divisor of \( v \) such that:

1. For each prime \( p \mid (v/u) \), we have \( \#R_p/E > \#R_p/p^2D_K \).
2. For each prime \( p \mid u \), we have \( \#R_p/(u/p)^2D_K > \#R_p/E \).

Certificate size is \( O(\log^{2+\epsilon} q) \).

Note that either \( D_1u^2D_K \) or \( D_1 = (u/p)^2D_K \).

We always have \( D_1 \leq D \). Very useful when \( D \ll D_\pi \).

This yields an algorithm to compute \( u \) with complexity

\[
L[1/2 + o(1), 1](|D|) + L[1/3, c](q)
\]

which depends primarily on \( D \), not \( q \).