Explicit Complex Multiplication

Benjamin Smith

INRIA Saclay–Île-de-France
& Laboratoire d'Informatique de l'École polytechnique (LIX)

Eindhoven, September 2008
So, where were we?

In the last lecture, we saw that if $E$ is an elliptic curve and $\text{End}(E)$ is its endomorphism ring, then

- $\text{End}(E)$ contains the multiplication-by-$m$ map for every $m$ in $\mathbb{Z}$;
- over $\mathbb{F}_q$, we also have the Frobenius endomorphism;
- we also have $\text{Aut}(E) \subset \text{End}(E)$
  (but generically $\text{Aut}(E) = \{[\pm 1]\}$, so this doesn’t give anything new.)

In this lecture, we want to explore the structure of $\text{End}(E)$.

We use $\text{End}(E)$ to denote the ring of endomorphisms of $E$ defined over $k$, while $\text{End}_{\overline{k}}(E)$ denotes the endomorphisms of $E$ defined over $\overline{k}$. 
More on the $j$-invariant

First, let’s talk a bit more about the $j$-invariant...

The idea is that there is essentially only one degree of freedom when choosing an elliptic curve over $\mathbb{F}_q$. Choosing a $j$-invariant and a twist determines your curve and your security.

Choosing the model of your curve makes a difference to your speed, but not your essential cryptographic efficiency.
The structure of $\text{End}(E)$

There are only three kinds of rings that $\text{End}(E)$ can be isomorphic to.

**Theorem**

Let $E$ be an elliptic curve over $k$. One of the following holds:

1. $\text{End}(E) = \text{End}_k(E) \cong \mathbb{Z}$.
2. $\text{End}_k(E) \cong \text{an order in a quadratic imaginary extension of } \mathbb{Q}$.
3. $\text{End}_k(E) \cong \text{an order in a quaternion algebra over } \mathbb{Q}$.

- If $\text{char } k = 0$, then (3) cannot occur (for slightly tricky reasons).
- If $\text{char } k \neq 0$, then (1) cannot occur (because $\pi_E$ is not an integer). Further, (3) occurs if and only if $E$ is supersingular.

If $\text{End}(E) \neq \mathbb{Z}$, then we say that $E$ has **complex multiplication** (CM). You should recognise $\mathbb{Z}$, but what about the other rings?
Orders in quadratic imaginary fields

Suppose \( K = \mathbb{Q}(\alpha) \) is a quadratic imaginary field (so \( \alpha \) satisfies a quadratic minimal polynomial with negative discriminant.)

The **ring of integers** (or **maximal order**) of \( K \) is

\[
\mathcal{O}_K = \{ \beta \in K : m(\beta) = 0 \text{ for some monic integer polynomial } m \}.
\]

The **orders** of \( K \) are the subrings \( \mathcal{O} \) of \( K \) satisfying

- \( \mathcal{O} \) is a finitely generated \( \mathbb{Z} \)-module, and
- \( \mathcal{O} \otimes \mathbb{Q} = K \) (that is, \( K \) is like \( \mathcal{O} \) “with (rational) denominators”).

These orders are precisely the subrings of \( K \) of the form

\[
\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K \quad \text{where } f^2 \text{ divides } \Delta_K \text{ (the discriminant of } K).\]
Orders in quadratic imaginary fields

Example

If $K = \mathbb{Q}(\sqrt{-3})$, then $(1 + \sqrt{-3})/2$ has minimal polynomial $X^2 - X + 1$, so $(1 + \sqrt{-3})/2$ is in $\mathcal{O}_K$.
In fact $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{-3})/2]$, and $\Delta_K = 12 = 2^2 \cdot 3$.
The orders of $K$ are therefore

$$\mathbb{Z} + 1 \cdot \mathcal{O}_K = \mathcal{O}_K \quad \text{and} \quad \mathbb{Z} + 2 \cdot \mathcal{O}_K = \mathbb{Z}[\sqrt{-3}].$$

Note that $\mathbb{Z}[\sqrt{-3}]$ has index 2 in $\mathcal{O}_K$. 
Orders in quaternion algebras

A **quaternion algebra** is an algebra of the form

\[ K = \mathbb{Q} + \mathbb{Q} \alpha + \mathbb{Q} \beta + \mathbb{Q} \alpha \beta \]

where \( \alpha^2 \) and \( \beta^2 \) are negative rational numbers, and \( \alpha \beta = -\beta \alpha \).

An order \( \mathcal{O} \) of \( K \) is a subring of \( K \) such that

- \( \mathcal{O} \) is finitely generated as a \( \mathbb{Z} \)-module, and
- \( \mathcal{O} \otimes \mathbb{Q} = K \) (that is, \( K \) is like \( \mathcal{O} \) “with denominators”).

We won’t be needing these today, since we will be concentrating on ordinary curves.
Frobenius

Let $E$ be an elliptic curve over $\mathbb{F}_q$, with Frobenius endomorphism $\pi_E$. Recall that $\pi_E$ has a characteristic polynomial

$$\chi_E(X) = X^2 - t_EX + q \quad \text{with} \quad |t_E| \leq 2\sqrt{q}$$

such that $\chi_E(\pi_E) = 0$.

The discriminant of $\chi_E$ is $\Delta = t_E^2 - 4q < 0$,
so $\mathbb{Q}(\pi_E) \cong \mathbb{Q}[X]/(\chi_E(X))$ is a quadratic imaginary field,
and $\text{End}(E)$ is an order in $\mathbb{Q}(\pi_E)$.

We have

$$\mathbb{Z}[\pi_E] \subset \text{End}(E) \subset \text{End}_k(E) \subset \mathcal{O}_{\mathbb{Q}(\pi_E)}.$$
Isogenies and endomorphism rings

Suppose $\phi : E \to F$ is an isogeny. How are $\text{End}(E)$ and $\text{End}(F)$ related?

**Definition**

If $E$ is an elliptic curve, then we define $\text{End}^0(E) := \text{End}(E) \otimes \mathbb{Q}$. We call $\text{End}^0(E)$ the **endomorphism algebra** of $E$.

For each $\psi$ in $\text{End}(F)$, we have an endomorphism $\phi^\dagger \psi \phi$ of $E$.

**Exercise**

Show that the map

$$\psi \mapsto \frac{1}{\deg(\phi)} \phi^\dagger \psi \phi$$

defines an isomorphism $\text{End}^0(F) \to \text{End}^0(E)$.

**Theorem**

$\text{End}^0(E)$ is an isogeny class invariant.
Corollary

If \( k = \mathbb{F}_q \), then \( \mathbb{Q}(\pi_E) \cong \mathbb{Q}(\pi_F) \).

Corollary

The set of supersingular elliptic curves over \( \mathbb{F}_p \) is an isogeny class.

If \( \phi : E \to F \) is an isogeny, then \( \text{End}^0(E) \cong \text{End}^0(F) \), but we can still have \( \text{End}(E) \not\cong \text{End}(F) \).
In particular, \( \text{End}(E) \) and \( \text{End}(F) \) can be different orders in \( \text{End}^0(E) \).

However, if \( \phi \) is an \( l \)-isogeny (that is, it has degree \( l \)), then either
- \( \text{End}(E) = \text{End}(F) \), or
- \( \text{End}(E) \) has index \( l \) in \( \text{End}(F) \), or
- \( \text{End}(F) \) has index \( l \) in \( \text{End}(E) \).

So an isogeny \( \phi \) can change the size of the endomorphism, but only by an index depending on the degree of \( \phi \).
A (very) brief look at Kohel’s algorithm

Suppose we want to determine $\text{End}(E)$ for some ordinary $E$ over $\mathbb{F}_q$.

First, we compute $t_E = (q + 1) - \#E(\mathbb{F}_q)$; then $\chi_E = X^2 - t_EX + q$, so

$$\text{End}(E) = \mathbb{Z} + f \cdot \mathcal{O}_{\mathbb{Q}(\pi_E)}$$

for some $f$ dividing the conductor $m$ of $\mathbb{Z}[[\pi_E]]$ in $\mathcal{O}_{\mathbb{Q}(\pi_E)}$.

Next, we factor $m$ (which is likely to be smooth, hence easy to factor).

For each prime $l$ dividing $m$, we construct the $l$-isogeny graph containing $j(E)$ in the moduli space, which looks something like this:
Kohel’s algorithm (continued)

The idea is that the $j$-invariants in the cycle correspond to curves $F$ with endomorphism ring $\text{End}(F) \cong \mathcal{O}_\mathbb{Q}(\pi_E)$, while each step away from the cycle reduces the endomorphism ring by an index $l$.

The largest power of $l$ dividing $f$ is the distance from $j(E)$ to the cycle.

Morain and Fouquet use these ideas in reverse to speed up the Schoof point counting algorithm.
What is the situation for elliptic curves over $\mathbb{Q}$?

If $E$ is an elliptic curve over $\mathbb{Q}$ (or $\mathbb{C}$ for that matter), then either

- $\text{End}(E) = \mathbb{Z}$ (the generic situation), or
- $\text{End}(E) \cong$ an order in a quadratic imaginary field (the exceptional case).

Remark

Over $\mathbb{C}$, elliptic curves are isomorphic to complex tori: that is, each curve is a quotient of $\mathbb{C}$ by a lattice $\Lambda = \langle 1, \tau \rangle$. The endomorphisms of $\mathbb{C}/\Lambda$ are the elements $z \in \mathbb{C}$ such that $z\Lambda = \Lambda$. Noninteger endomorphisms can only exist if $\tau$ is an algebraic integer, and in fact all of these endomorphisms must lie in $\mathbb{Q}(\tau)$. 

Reduction of curves and endomorphisms

Recall that if $E : y^2 = f(x)$ is an elliptic curve defined over $\mathbb{Q}$ and $p$ is a prime of good reduction for $E$, then reducing the equation of $E$ modulo $p$ defines an elliptic curve $\overline{E} : y^2 = \overline{f}(x)$ over $\mathbb{F}_p$.

If $\phi$ is an endomorphism of $E$, then we can reduce the coefficients of its rational map modulo $p$ to give an endomorphism $\overline{\phi}$ of $\overline{E}$.

**Theorem**

The map $\text{End}(E) \to \text{End}(\overline{E})$ induced by reducing modulo $p$ is an injective homomorphism.

Many curves over $\mathbb{Q}$ reduce to the same $\overline{E}$ modulo $p$, and $\text{End}(\overline{E})$ “contains” the endomorphism ring of every one of them.
The endomorphism algebra of a reduction

Corollary

Let $E$ be an elliptic curve over $\mathbb{Q}$ such that $\text{End}(E)$ is an order $\mathcal{O}$ in a quadratic imaginary field $K$, and let $p$ be any prime of good reduction for $E$. Then $\text{End}(\overline{E})$ contains a subring isomorphic to $\mathcal{O}$.

Note that $\text{End}^0(E)$ need not be isomorphic to $K$. If $\overline{E}$ is ordinary then $\text{End}^0(E) \cong K$, but if $\overline{E}$ is supersingular then $K$ is only the center of $\text{End}^0(E)$. 
The CM method for curve construction

One application of this result is the CM method (of which we will only give a very rough sketch).

Suppose we have an algorithm that, given a quadratic imaginary field $K$, together with an element $\alpha$ of $K$ of norm $p$, constructs an elliptic curve $E$ over $\mathbb{Q}$ such that $\text{End}^0(E) \cong K$ with $\alpha$ representing $\pi_E$.

Suppose now that we want a curve $F$ over $\mathbb{F}_p$ such that $\#F(\mathbb{F}_p) = N$. We know that $t_E = p + 1 - N$, so $\text{End}^0(F)$ must contain the field $K = \mathbb{Q}[X]/(X^2 - (p + 1 - N)X + p)$.

Applying the algorithm we compute a curve $E$ over $\mathbb{Q}$ with $\text{End}^0(E) \cong K$. Then we reduce $E$ modulo $p$ to obtain a curve $F = \overline{E}$ over $\mathbb{F}_p$ with the required number of points.

(More generally, $E$ could be defined over a number field.)
Class polynomials

It remains to determine a way to compute an $E$ over $\mathbb{Q}$.

It is enough to compute the $j$-invariant of $E$, since this is enough to reconstruct $E$ (though we may need to check the right twist of $\overline{E}$.)

The conventional solution uses the **class polynomial** of $K$: that is, a polynomial $H_{\Delta_K}(X)$ whose roots are the $j$-invariants of curves over $\mathbb{Q}$ whose endomorphism ring is equal to $\mathcal{O}_K$.

These class polynomials can be precomputed relatively easily: Enge’s algorithm runs in essentially linear time in size of $\Delta_K$. The hard part is finding enough disk space to write down the polynomial.

In Magma, you can compute class polynomials using
\[ \text{HilbertClassPolynomial}(\text{Discriminant}(K)); \]
Examples of class polynomials

Example
Let $K = \mathbb{Q}(i) = \mathbb{Q}[X]/(X^2 + 1)$. The maximal order of $K$ is $\mathbb{Z}[i]$. The field $K$ has discriminant $-4$. The class polynomial of $K$ is $H_{-4}(X) = X - 1728$; so only curves with $j$-invariant 1728 can have endomorphism ring isomorphic to $\mathbb{Z}[i]$. Recall that these curves are all $\overline{\mathbb{Q}}$-isomorphic to $E : y^2 = x^3 + x$.

Example
Some examples of other class polynomials include

$$H_{-20}(X) = X^2 - 1264000X - 681472000$$

$$H_{-52}(X) = X^2 - 6896880000X - 567663552000000$$

$$H_{-31}(X) = X^3 + 39491307X^2 - 58682638134X + 1566028350940383$$
Eigenvalues of endomorphisms

Let $E$ be an elliptic curve over $\mathbb{F}_q$, and suppose $E(\mathbb{F}_q)$ has a subgroup $G$ of large prime order $N$ (so $N^2$ does not divide $\#E(\mathbb{F}_q)$).

For cryptography, we need to do a lot of scalar multiplication in $G$.

Suppose we can efficiently compute a non-integer endomorphism $\phi$ of $E$; let $m_\phi(X)$ be its (quadratic) minimal polynomial.

We have $\phi(G) = G$; but $G$ is cyclic, so its endomorphisms are all integer multiplications; so $\phi$ acts like an integer eigenvalue on $G$. Indeed, $\phi$ acts like $[\lambda]$ on $G$, where $\lambda$ is one of the roots of $m_\phi(X) \mod N$.

Given an integer $m$, we can write

$$[m] = [a] + [\lambda][b]$$

with $a$ and $b$ about half the size of $m$.

For any $P$ in $G$, we can then compute $[m]P$ more efficiently by using

$$[m]P = [a]P + \phi([b]P).$$

This is the basis of Gallant–Lambert–Vanstone (GLV) multiplication.
Other fast multiplication techniques

Endomorphisms also appear in other fast multiplication techniques.

Example (Multiplication with Frobenius expansions)

Let $E$ be an elliptic curve defined over $\mathbb{F}_p$, but viewed as an elliptic curve over $\mathbb{F}_q$ where $q = p^n$. The $p$-power Frobenius isogeny is then an endomorphism $\pi_p$ of $E$. Again, $\pi_p(G) = G$, so $\pi_p$ has an eigenvalue $\lambda$ on $G$.

When we want to multiply by an integer $m$, we can expand $m$ in base $\lambda$, writing

$$m = m_0 + m_1 \lambda + m_2 \lambda^2 + \cdots$$

and then evaluate

$$[m]P = [m_0]P + \pi_p([m_1]P) + \pi_p^2([m_2]P) + \cdots.$$