Computing isogenies

John Cremona

University of Warwick

24 June 2010

Introduction

In this lecture we will look at ways of finding isogenies between elliptic curves.

Many of the methods we will describe work in complete generality. However, the situation for curves over finite fields (and more generally, in characteristic p) has many very different features.

Hence we assume for this lecture that K is a field of characteristic zero, and usually that K is an algebraic number field (including $\mathbb{Q}$).

The two basic problems

1. Given two elliptic curves E_1, E_2 defined over K, determine whether or not E_1 and E_2 are isogenous ($E_1 \sim E_2$)

The two basic problems

1. Given two elliptic curves E_1, E_2 defined over K, determine whether or not E_1 and E_2 are isogenous ($E_1 \sim E_2$)
2. Given one elliptic curve E defined over K, find "all" elliptic curves over K which are isogenous to E over K.

The two basic problems

1. Given two elliptic curves E_1, E_2 defined over K, determine whether or not E_1 and E_2 are isogenous ($E_1 \sim E_2$)
2. Given one elliptic curve E defined over K, find "all" elliptic curves over K which are isogenous to E over K.

Note: isogeny (over K) is an equivalence relation; the second problem is to find the *isogeny class* containing a given curve. This is a finite set when K is a number field (we only count curves up to isomorphism).

The two basic problems

1. Given two elliptic curves E_1, E_2 defined over K, determine whether or not E_1 and E_2 are isogenous ($E_1 \sim E_2$)
2. Given one elliptic curve E defined over K, find “all” elliptic curves over K which are isogenous to E over K.

Note: isogeny (over K) is an equivalence relation; the second problem is to find the *isogeny class* containing a given curve. This is a finite set when K is a number field (we only count curves up to isomorphism).

The first problem is to detect when two curves belong to the same class.

What is an isogeny?

See Silverman III.4

Let E_1, E_2 be elliptic curves defined over K. An *isogeny* from E_1 to E_2 defined over K is a morphism of curves $\varphi : E_1 \to E_2$ defined over K such that $\varphi(O_{E_1}) = O_{E_2}$.

E_1 and E_2 are *isogenous* if there exists a non-zero isogeny between them.

What is an isogeny?

See Silverman III.4

Let E_1, E_2 be elliptic curves defined over K. An *isogeny* from E_1 to E_2 defined over K is a morphism of curves $\varphi : E_1 \to E_2$ defined over K such that $\varphi(O_{E_1}) = O_{E_2}$.

E_1 and E_2 are *isogenous* if there exists a non-zero isogeny between them.

- Isogenies are automatically group homomorphisms
- If $\varphi \neq 0$ then $\ker \varphi$ is a *finite* subgroup of $E(\overline{K})$, whose order is the *degree* $\deg \varphi$ (the degree of φ as a curve morphism).

  $\operatorname{char} K = 0$ so we do not need to mention separability!
- Isogeny is an equivalence relation: if $\varphi \neq 0$ there is a *dual isogeny* $\hat{\varphi} : E_2 \to E_1$ of the same degree

More facts about isogenies

- The set of all isogenies $E_1 \to E_2$ is an abelian group denoted $\mathrm{Hom}(E_1, E_2)$ ($= 0$ unless the E_j are isogenous)
- The multiplication maps $[m] : E \to E$ are isogenies
- Every nonzero isogeny $\varphi : E_1 \to E_2$ factors uniquely as

$$E_1 \xrightarrow{[m]} E_1 \xrightarrow{\varphi'} E_2$$

  where φ' has *cyclic* kernel.
- Every cyclic isogeny $\varphi : E_1 \to E_2$ factors uniquely as a product of (cyclic) isogenies of *prime* degree.

So in looking for isogenies from E_1 to other curves we may restrict to ℓ-isogenies: *cyclic isogenies of prime degree ℓ*.

Problem 1: isogeny testing

1. Given two elliptic curves E_1, E_2 defined over a number field K, determine whether or not E_1 and E_2 are isogenous.

This is one of those problems where if the answer is “no”, this is easy to discover, but if the answer is “yes” it is a lot harder to prove!

Problem 1: isogeny testing

1. Given two elliptic curves E_1, E_2 defined over a number field K, determine whether or not E_1 and E_2 are isogenous.

This is one of those problems where if the answer is “no”, this is easy to discover, but if the answer is “yes” it is a lot harder to prove! (Think of primality testing!)

Problem 1: isogeny testing

1. Given two elliptic curves E_1, E_2 defined over a number field K, determine whether or not E_1 and E_2 are isogenous.

This is one of those problems where if the answer is “no”, this is easy to discover, but if the answer is “yes” it is a lot harder to prove! (Think of primality testing!)

- Isogenous curves have the same conductor $\mathcal{N}$, which is easy to compute. Answer “no” if $\mathcal{N}_{E_1} \neq \mathcal{N}_{E_2}$.

Problem 1: isogeny testing

1. Given two elliptic curves E_1, E_2 defined over a number field K, determine whether or not E_1 and E_2 are isogenous.

This is one of those problems where if the answer is “no”, this is easy to discover, but if the answer is “yes” it is a lot harder to prove! (Think of primality testing!)

- Isogenous curves have the same conductor $\mathcal{N}$, which is easy to compute. Answer “no” if $\mathcal{N}_{E_1} \neq \mathcal{N}_{E_2}$.
- Isogenous curves are “locally isogenous”: they have the same number of points modulo $\mathfrak{p}$ for all primes $\mathfrak{p}$. Test this for several primes, and answer “no” if any disagree.

Isogeny testing, continued

Now we have two curves which look isogenous, in the sense that they have the same conductor and the same number of points modulo $\mathfrak{p}$ for many small primes $\mathfrak{p}$.

Isogeny testing, continued

Now we have two curves which look isogenous, in the sense that they have the same conductor and the same number of points modulo $\mathfrak{p}$ for many small primes $\mathfrak{p}$.

In other words, their L-series look the same (many Euler factors agree).

Isogeny testing, continued

Now we have two curves which look isogenous, in the sense that they have the same conductor and the same number of points modulo $\mathfrak{p}$ for many small primes $\mathfrak{p}$.

In other words, their L-series look the same (many Euler factors agree).

What next?

Isogeny testing, continued

Now we have two curves which look isogenous, in the sense that they have the same conductor and the same number of points modulo $\mathfrak{p}$ for many small primes $\mathfrak{p}$.

In other words, their L-series look the same (many Euler factors agree).

What next?

- Find the complete isogeny class of E_1 and see if it contains E_2 (up to isomorphism): see problem 2!

Isogeny testing, continued

Now we have two curves which look isogenous, in the sense that they have the same conductor and the same number of points modulo $\mathfrak{p}$ for many small primes $\mathfrak{p}$.

In other words, their L-series look the same (many Euler factors agree).

What next?

- Find the complete isogeny class of E_1 and see if it contains E_2 (up to isomorphism): see problem 2!
- Or just compute chains of ℓ-isogenies for $\ell = 2, 3, 5, \ldots$ and hope for the best.

Problem 2: finding the complete isogeny class

This divides into two separate sub-problems:

Problem 2: finding the complete isogeny class

This divides into two separate sub-problems:

1. Given an elliptic curve E and a specific prime ℓ, find all curves ℓ-isogenous to E

Problem 2: finding the complete isogeny class

This divides into two separate sub-problems:

1. Given an elliptic curve E and a specific prime ℓ, find all curves ℓ-isogenous to E
2. Given an elliptic curve E, determine for which primes ℓ there exists an ℓ-isogeny from E

Problem 2: finding the complete isogeny class

This divides into two separate sub-problems:

1. Given an elliptic curve E and a specific prime ℓ, find all curves ℓ-isogenous to E
2. Given an elliptic curve E, determine for which primes ℓ there exists an ℓ-isogeny from E

Sub-problem 2 is quite deep. The list of ℓ which occur for elliptic curves over $\mathbb{Q}$ was determined by Mazur in his famous 1978 paper "Rational Isogenies of prime degree":

$$\ell \in \{2, 3, 5, 7, 13\} \cup \{11, 17, 37\} \cup \{11, 19, 43, 67, 163\}$$

Problem 2: finding the complete isogeny class

This divides into two separate sub-problems:

1. Given an elliptic curve E and a specific prime ℓ, find all curves ℓ-isogenous to E
2. Given an elliptic curve E, determine for which primes ℓ there exists an ℓ-isogeny from E

Sub-problem 2 is quite deep. The list of ℓ which occur for elliptic curves over $\mathbb{Q}$ was determined by Mazur in his famous 1978 paper "Rational Isogenies of prime degree":

$$\ell \in \{2, 3, 5, 7, 13\} \cup \{11, 17, 37\} \cup \{11, 19, 43, 67, 163\}$$

No such list is known for any other number field!

We will concentrate on sub-problem 1.

Isogeny kernels

Let $\varphi : E \to E'$ be an ℓ-isogeny defined over K. The kernel $H = \ker \varphi$ is a cyclic subgroup of $E(\overline{K})$ which is defined over K.

Isogeny kernels

Let $\varphi : E \to E'$ be an ℓ-isogeny defined over K. The kernel $H = \ker \varphi$ is a cyclic subgroup of $E(\overline{K})$ which is defined over K. This means that it is stable under Galois, i.e. that

$$P \in H \implies P^\sigma \in H \qquad \forall \sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$$

Isogeny kernels

Let $\varphi : E \to E'$ be an ℓ-isogeny defined over K. The kernel $H = \ker \varphi$ is a cyclic subgroup of $E(\overline{K})$ which is defined over K. This means that it is stable under Galois, i.e. that

$$P \in H \implies P^\sigma \in H \qquad \forall \sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$$

Note that this does *not* mean that $H \subset E(K)$!

Isogeny kernels

Let $\varphi : E \to E'$ be an ℓ-isogeny defined over K. The kernel $H = \ker \varphi$ is a cyclic subgroup of $E(\overline{K})$ which is defined over K. This means that it is stable under Galois, i.e. that

$$P \in H \implies P^\sigma \in H \qquad \forall \sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$$

Note that this does *not* mean that $H \subset E(K)$! But is does mean that the *kernel polynomial* $\Psi_H(X) \in K[X]$,

Isogeny kernels

Let $\varphi : E \to E'$ be an ℓ-isogeny defined over K. The kernel $H = \ker \varphi$ is a cyclic subgroup of $E(\overline{K})$ which is defined over K. This means that it is stable under Galois, i.e. that

$$P \in H \implies P^\sigma \in H \qquad \forall \sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$$

Note that this does *not* mean that $H \subset E(K)$! But is does mean that the *kernel polynomial* $\Psi_H(X) \in K[X]$, where

$$\Psi_H(X) = \prod_{\pm P = (x_P, y_P) \in H \setminus \{O\}} (X - x_P).$$

In this product, we only take one of each pair $\pm P$, so Ψ_H has distinct roots and degree $(\ell - 1)/2$ (or degree 1 when $\ell = 2$).

Isogeny kernels

Let $\varphi : E \to E'$ be an ℓ-isogeny defined over K. The kernel $H = \ker\varphi$ is a cyclic subgroup of $E(\overline{K})$ which is defined over K. This means that it is stable under Galois, i.e. that

$$P \in H \implies P^\sigma \in H \qquad \forall \sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$$

Note that this does *not* mean that $H \subset E(K)$! But is does mean that the *kernel polynomial* $\Psi_H(X) \in K[X]$, where

$$\Psi_H(X) = \prod_{\pm P = (x_P, y_P) \in H \setminus \{O\}} (X - x_P).$$

In this product, we only take one of each pair $\pm P$, so Ψ_H has distinct roots and degree $(\ell - 1)/2$ (or degree 1 when $\ell = 2$). Given Ψ_H there are standard formulas to compute both φ and the codomain curve $E' = E/H$. So we will concentrate on finding Ψ_H.

Division polynomials

Nonzero points in the kernel of an ℓ-isogeny all have order ℓ, since $[\ell] = \hat{\varphi} \circ \varphi$ (and ℓ is prime).

Division polynomials

Nonzero points in the kernel of an ℓ-isogeny all have order ℓ, since $[\ell] = \hat{\varphi} \circ \varphi$ (and ℓ is prime).

Hence the kernel polynomial $\Psi_H(X)$ is a factor of the ℓ-*division polynomial* which can be defined as $\Psi_l(X) = \Psi_{E[\ell]}(X)$;

Division polynomials

Nonzero points in the kernel of an ℓ-isogeny all have order ℓ, since $[\ell] = \hat{\varphi} \circ \varphi$ (and ℓ is prime).

Hence the kernel polynomial $\Psi_H(X)$ is a factor of the ℓ-*division polynomial* which can be defined as $\Psi_l(X) = \Psi_{E[\ell]}(X)$; it has degree $(\ell^2 - 1)/2$ (or 3 when $\ell = 2$) and coefficients in K.

Division polynomials

Nonzero points in the kernel of an ℓ-isogeny all have order ℓ, since $[\ell] = \hat{\varphi} \circ \varphi$ (and ℓ is prime).

Hence the kernel polynomial $\Psi_H(X)$ is a factor of the ℓ-*division polynomial* which can be defined as $\Psi_l(X) = \Psi_{E[\ell]}(X)$; it has degree $(\ell^2 - 1)/2$ (or 3 when $\ell = 2$) and coefficients in K.

Over $\overline{K}$, the division polynomial $\Psi_l(X)$ factors as a product of exactly $l + 1$ (possibly reducible) kernel polynomials.

Division polynomials

Nonzero points in the kernel of an ℓ-isogeny all have order ℓ, since $[\ell] = \hat{\varphi} \circ \varphi$ (and ℓ is prime).

Hence the kernel polynomial $\Psi_H(X)$ is a factor of the ℓ-*division polynomial* which can be defined as $\Psi_l(X) = \Psi_{E[\ell]}(X)$; it has degree $(\ell^2 - 1)/2$ (or 3 when $\ell = 2$) and coefficients in K.

Over $\overline{K}$, the division polynomial $\Psi_l(X)$ factors as a product of exactly $l + 1$ (possibly reducible) kernel polynomials. It is easy to see that E has exactly $\ell + 1$ different ℓ-isogenies, since that is the number of subgroups of order ℓ in $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$.

Division polynomials

Nonzero points in the kernel of an ℓ-isogeny all have order ℓ, since $[\ell] = \hat{\varphi} \circ \varphi$ (and ℓ is prime).

Hence the kernel polynomial $\Psi_H(X)$ is a factor of the ℓ-*division polynomial* which can be defined as $\Psi_l(X) = \Psi_{E[\ell]}(X)$; it has degree $(\ell^2 - 1)/2$ (or 3 when $\ell = 2$) and coefficients in K.

Over $\overline{K}$, the division polynomial $\Psi_l(X)$ factors as a product of exactly $l + 1$ (possibly reducible) kernel polynomials. It is easy to see that E has exactly $\ell + 1$ different ℓ-isogenies, since that is the number of subgroups of order ℓ in $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$.

Hence one approach is to factor $\Psi_l(X)$ over K and work out which irreducible factors combine to give valid kernel polynomials.

Division polynomials

Nonzero points in the kernel of an ℓ-isogeny all have order ℓ, since $[\ell] = \hat{\varphi} \circ \varphi$ (and ℓ is prime).

Hence the kernel polynomial $\Psi_H(X)$ is a factor of the ℓ-*division polynomial* which can be defined as $\Psi_l(X) = \Psi_{E[\ell]}(X)$; it has degree $(\ell^2 - 1)/2$ (or 3 when $\ell = 2$) and coefficients in K.

Over $\overline{K}$, the division polynomial $\Psi_l(X)$ factors as a product of exactly $l + 1$ (possibly reducible) kernel polynomials. It is easy to see that E has exactly $\ell + 1$ different ℓ-isogenies, since that is the number of subgroups of order ℓ in $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$.

Hence one approach is to factor $\Psi_l(X)$ over K and work out which irreducible factors combine to give valid kernel polynomials. This is straightforward when $\ell = 2$ or $\ell = 3$, when kernel polynomials have degree 1.

2-isogenies

The first easy case.

2-isogenies

The first easy case.

Let E have equation $Y^2 = X^3 + AX + B$. Then $\Psi_2(X) = X^3 + AX + B$.

2-isogenies

The first easy case.

Let E have equation $Y^2 = X^3 + AX + B$. Then $\Psi_2(X) = X^3 + AX + B$.

To each root x_0 of $\Psi_2(X)$ in K we have a point $P = (x_0, 0)$ of order 2 and subgroup $H = \langle P \rangle = \{O_E, P\}$.

2-isogenies

The first easy case.

Let E have equation $Y^2 = X^3 + AX + B$. Then $\Psi_2(X) = X^3 + AX + B$.

To each root x_0 of $\Psi_2(X)$ in K we have a point $P = (x_0, 0)$ of order 2 and subgroup $H = \langle P \rangle = \{O_E, P\}$.

The kernel polynomial is $X - x_0$, and the isogenous curve $E' = E/H$ has equation

$$E' : Y^2 = X^3 + (A - 5(3x_0^2 + A))X + (B - 7x_0(3x_0^2 + A)).$$

2-isogenies

The first easy case.

Let E have equation $Y^2 = X^3 + AX + B$. Then $\Psi_2(X) = X^3 + AX + B$.

To each root x_0 of $\Psi_2(X)$ in K we have a point $P = (x_0, 0)$ of order 2 and subgroup $H = \langle P \rangle = \{O_E, P\}$.

The kernel polynomial is $X - x_0$, and the isogenous curve $E' = E/H$ has equation

$$E' : Y^2 = X^3 + (A - 5(3x_0^2 + A))X + (B - 7x_0(3x_0^2 + A)).$$

For a general Weierstrass equation the formulas are not much more complicated.

3-isogenies

The second easy case.

3-isogenies

The second easy case. Let E have equation $Y^2 = X^3 + AX + B$.
Then $\Psi_3(X) = 3X^4 + 6AX^2 + 12BX - A^2$.

3-isogenies

The second easy case. Let E have equation $Y^2 = X^3 + AX + B$. Then $\Psi_3(X) = 3X^4 + 6AX^2 + 12BX - A^2$.

To each root x_0 of $\Psi_3(X)$ in K we have a pair of points $P = (x_0, \pm y_0)$ of order 3 and subgroup $H = \langle P \rangle = \{O_E, P, -P\}$.

3-isogenies

The second easy case. Let E have equation $Y^2 = X^3 + AX + B$. Then $\Psi_3(X) = 3X^4 + 6AX^2 + 12BX - A^2$.

To each root x_0 of $\Psi_3(X)$ in K we have a pair of points $P = (x_0, \pm y_0)$ of order 3 and subgroup $H = \langle P \rangle = \{O_E, P, -P\}$.

The kernel polynomial is again $X - x_0$, and the isogenous curve $E' = E/H$ has equation

$$E' : Y^2 = X^3 - 3(3A + 10x_0^2)X - (70x_0^3 + 42Ax_0 + 27B).$$

Strategies for larger ℓ

We have several strategies for handling larger ℓ:

Strategies for larger ℓ

We have several strategies for handling larger ℓ:

1. Using period lattices and floating point arithmetic.

Strategies for larger ℓ

We have several strategies for handling larger ℓ:

1. Using period lattices and floating point arithmetic. I have used this for years over $\mathbb{Q}$, and it is fast and efficient, but suffers from the need to use sufficiently high precision.

Strategies for larger ℓ

We have several strategies for handling larger ℓ:

1. Using period lattices and floating point arithmetic. I have used this for years over $\mathbb{Q}$, and it is fast and efficient, but suffers from the need to use sufficiently high precision. Over other number fields it would be possible in principle (working with all the embeddings $K \hookrightarrow \mathbb{C}$) but messy.

Strategies for larger ℓ

We have several strategies for handling larger ℓ:

1. Using period lattices and floating point arithmetic. I have used this for years over $\mathbb{Q}$, and it is fast and efficient, but suffers from the need to use sufficiently high precision. Over other number fields it would be possible in principle (working with all the embeddings $K \hookrightarrow \mathbb{C}$) but messy.
2. The modular approach

Strategies for larger ℓ

We have several strategies for handling larger ℓ:

1. Using period lattices and floating point arithmetic. I have used this for years over $\mathbb{Q}$, and it is fast and efficient, but suffers from the need to use sufficiently high precision. Over other number fields it would be possible in principle (working with all the embeddings $K \hookrightarrow \mathbb{C}$) but messy.
2. The modular approach
3. Factoring division polynomials (carefully!)

Strategies for larger ℓ

We have several strategies for handling larger ℓ:

1. Using period lattices and floating point arithmetic. I have used this for years over $\mathbb{Q}$, and it is fast and efficient, but suffers from the need to use sufficiently high precision. Over other number fields it would be possible in principle (working with all the embeddings $K \hookrightarrow \mathbb{C}$) but messy.
2. The modular approach
3. Factoring division polynomials (carefully!)

Ignoring the first approach, I describe the others, starting with the case $\ell = 5$.

5-isogenies via division polynomials

Joint work with Kimi Tsukazaki

The 5-division polynomial $\Psi_5(X)$ has degree 12; the 6 kernel polynomials are now *quadratic* factors.

5-isogenies via division polynomials

Joint work with Kimi Tsukazaki

The 5-division polynomial $\Psi_5(X)$ has degree 12; the 6 kernel polynomials are now *quadratic* factors.

Not every quadratic factor is a kernel polynomial!

5-isogenies via division polynomials

Joint work with Kimi Tsukazaki

The 5-division polynomial $\Psi_5(X)$ has degree 12; the 6 kernel polynomials are now *quadratic* factors.

Not every quadratic factor is a kernel polynomial!

Each kernel now has the form $H = \{O, \pm P, \pm 2P\}$ and the two roots of the kernel polynomial are $x(\pm P), x(\pm 2P)$.

5-isogenies via division polynomials

Joint work with Kimi Tsukazaki

The 5-division polynomial $\Psi_5(X)$ has degree 12; the 6 kernel polynomials are now *quadratic* factors.

Not every quadratic factor is a kernel polynomial!

Each kernel now has the form $H = \{O, \pm P, \pm 2P\}$ and the two roots of the kernel polynomial are $x(\pm P), x(\pm 2P)$.

Let $m_2(X)$ be the degree 4 rational function such that $x(2P) = m_2(x(P))$ for all $P \in E(\overline{K})$. The condition for a quadratic factor $f(X)$ of $\Psi_5(X)$ to be a kernel polynomial is that

$$f(x_0) = 0 \implies f(m_2(x_0)) = 0.$$

5-isogenies via division polynomials (continued)

For $f(X) \in K[X]$ define an operation $f \mapsto \mu(f)$ by

$$\mu(f)(X) = \gcd(\Psi_\ell(X), \mathrm{num}(f(m_2(X))))$$

(where $\mathrm{num}()$ denotes the numerator of a rational function).

5-isogenies via division polynomials (continued)

For $f(X) \in K[X]$ define an operation $f \mapsto \mu(f)$ by

$$\mu(f)(X) = \gcd(\Psi_\ell(X), \mathrm{num}(f(m_2(X))))$$

(where $\mathrm{num}()$ denotes the numerator of a rational function). Now, a quadratic factor $f(X)$ of $\Psi_5(X)$ is a kernel polynomial if and only if $\mu(f) = f$.

5-isogenies via division polynomials (continued)

For $f(X) \in K[X]$ define an operation $f \mapsto \mu(f)$ by

$$\mu(f)(X) = \gcd(\Psi_\ell(X), \mathrm{num}(f(m_2(X))))$$

(where $\mathrm{num}()$ denotes the numerator of a rational function).
Now, a quadratic factor $f(X)$ of $\Psi_5(X)$ is a kernel polynomial if and only if $\mu(f) = f$.

Any linear factors of $\Psi_5(X)$ are permuted in pairs by μ: we get a kernel polynomial by taking products $f(X)\mu(f(X))$ with one f from each such pair, or from a quadratic factor f with $\mu(f) = f$.

ℓ-isogenies via division polynomials: the general case

Let ℓ be any odd prime. Assume that 2 generates $(\mathbb{Z}/\ell\mathbb{Z})^*/\{\pm 1\}$ (i.e., 2 is a “semi-primitive root modulo ℓ).

ℓ-isogenies via division polynomials: the general case

Let ℓ be any odd prime. Assume that 2 generates $(\mathbb{Z}/\ell\mathbb{Z})^*/\{\pm 1\}$ (i.e., 2 is a “semi-primitive root modulo ℓ).

1. Factor $\Psi_l(X)$. Discard any irreducible factors whose degree does not divide $(\ell - 1)/2$, and consider the remaining factors f in turn.

ℓ-isogenies via division polynomials: the general case

Let ℓ be any odd prime. Assume that 2 generates $(\mathbb{Z}/\ell\mathbb{Z})^*/\{\pm 1\}$ (i.e., 2 is a “semi-primitive root modulo ℓ).

1. Factor $\Psi_l(X)$. Discard any irreducible factors whose degree does not divide $(\ell - 1)/2$, and consider the remaining factors f in turn.
2. Write $(\ell - 1)/2 = de$ where $d = \deg(f)$. Form in succession

$$f, \mu(f), \mu^2(f), \ldots, \mu^e(f)$$

(which are all irreducible factors of $\Psi_l(X)$).

ℓ-isogenies via division polynomials: the general case

Let ℓ be any odd prime. Assume that 2 generates $(\mathbb{Z}/\ell\mathbb{Z})^*/\{\pm 1\}$ (i.e., 2 is a “semi-primitive root modulo ℓ).

1. Factor $\Psi_l(X)$. Discard any irreducible factors whose degree does not divide $(\ell - 1)/2$, and consider the remaining factors f in turn.
2. Write $(\ell - 1)/2 = de$ where $d = \deg(f)$. Form in succession

$$f, \mu(f), \mu^2(f), \ldots, \mu^e(f)$$

(which are all irreducible factors of $\Psi_l(X)$).
3. If $\mu^e(f) \neq f$, discard all these factors: f fails.

ℓ-isogenies via division polynomials: the general case

Let ℓ be any odd prime. Assume that 2 generates $(\mathbb{Z}/\ell\mathbb{Z})^*/\{\pm 1\}$ (i.e., 2 is a "semi-primitive root modulo ℓ).

1. Factor $\Psi_l(X)$. Discard any irreducible factors whose degree does not divide $(\ell - 1)/2$, and consider the remaining factors f in turn.
2. Write $(\ell - 1)/2 = de$ where $d = \deg(f)$. Form in succession
$$f, \mu(f), \mu^2(f), \ldots, \mu^e(f)$$
(which are all irreducible factors of $\Psi_l(X)$).
3. If $\mu^e(f) \neq f$, discard all these factors: f fails.
Otherwise, f passes, and $g = \prod_{j=0}^{e-1} \mu^j(f)$ is the kernel of an ℓ-isogeny defined over K.

Why 2? When 2?

2 is a semi-primitive root modulo ℓ for

$$\ell = 3, 5, 7, 11, 13, 19, 23, 29, 37, 47, 53, 59, 61, 67, 71, 79, 83, \ldots$$

but not for

$$\ell = 17, 31, 41, 43, 73, 89, 97, \ldots$$

Why 2? When 2?

2 is a semi-primitive root modulo ℓ for

$$\ell = 3, 5, 7, 11, 13, 19, 23, 29, 37, 47, 53, 59, 61, 67, 71, 79, 83, \ldots$$

but not for

$$\ell = 17, 31, 41, 43, 73, 89, 97, \ldots$$

We can instead use any semi-primitive root a, replacing m_2 by the rational function m_a which gives the multiplication-by-a map on the x-coordinate. In fact, $a = 2$ or $a = 3$ work for all $\ell < 100$ except $\ell = 41, 73, 97$ for which $a = 6, 5, 5$ work.

Why 2? When 2?

2 is a semi-primitive root modulo ℓ for

$$\ell = 3, 5, 7, 11, 13, 19, 23, 29, 37, 47, 53, 59, 61, 67, 71, 79, 83, \ldots$$

but not for

$$\ell = 17, 31, 41, 43, 73, 89, 97, \ldots$$

We can instead use any semi-primitive root a, replacing m_2 by the rational function m_a which gives the multiplication-by-a map on the x-coordinate. In fact, $a = 2$ or $a = 3$ work for all $\ell < 100$ except $\ell = 41, 73, 97$ for which $a = 6, 5, 5$ work.

However, this method becomes rapidly more expensive for larger ℓ since both computing and factoring $\Psi_l(X)$ are slow: remember that the degree is $(\ell^2 - 1)/2$.

The modular method

Joint work with Mark Watkins and Kimi Tsukazaki

We have developed this method for $\ell = 5$, 7 and 13; it also works for $\ell = 2$ and 3 but then is no easier than the division polynomial method.

Why these primes?

The modular method

Joint work with Mark Watkins and Kimi Tsukazaki

We have developed this method for $\ell = 5$, 7 and 13; it also works for $\ell = 2$ and 3 but then is no easier than the division polynomial method.

Why these primes?

These are the prime values of ℓ for which the modular curve $X_0(\ell)$ has *genus* 0.

This means that the j-invariants of elliptic curves with a rational ℓ-isogeny can be expressed in terms of a single free parameter t, namely a generator for the function field of $X_0(\ell)$, of degree $l + 1$.

Fricke moduli for genus zero primes

As generators of the function fields of $X_0(\ell)$ we may take functions t satisfying

$$
\begin{aligned}
(\ell = 2) &\quad j = F_2(t) = (t+16)^3/t \\
(\ell = 3) &\quad j = F_3(t) = (t+3)^3(t+27)/t \\
(\ell = 5) &\quad j = F_5(t) = (t^2+10t+5)^3/t \\
(\ell = 7) &\quad j = F_7(t) = (t^2+5t+1)^3(t^2+13t+49)/t \\
(\ell = 13) &\quad j = F_{13}(t) = (t^2+5t+13)(t^4+7t^3+20t^2+19t+1)^3/t
\end{aligned}
$$

Why?

Brief explanation: Non-cuspidal points on $X_0(N)$ parametrize pairs (E, H) where E is an elliptic curve and H a cyclic subgroup of order N. When $N = 1$ we get the usual j-line. For larger N for which $X_0(N)$ has genus zero, we need a different modular function t, of level N, and the covering map $X_0(N) \to X_0(1)$ is given by a rational map $t \mapsto j = F(t)$.

Why?

Brief explanation: Non-cuspidal points on $X_0(N)$ parametrize pairs (E,H) where E is an elliptic curve and H a cyclic subgroup of order N. When $N=1$ we get the usual j-line. For larger N for which $X_0(N)$ has genus zero, we need a different modular function t, of level N, and the covering map $X_0(N) \to X_0(1)$ is given by a rational map $t \mapsto j = F(t)$.

This means that for a curve with given j-invariant, the isogenous curves (over K) correspond to the solutions $t \in K$ to the equation $F_\ell(t) = j$, of which there are at most $l+1$.

Why?

Brief explanation: Non-cuspidal points on $X_0(N)$ parametrize pairs (E, H) where E is an elliptic curve and H a cyclic subgroup of order N. When $N = 1$ we get the usual j-line. For larger N for which $X_0(N)$ has genus zero, we need a different modular function t, of level N, and the covering map $X_0(N) \to X_0(1)$ is given by a rational map $t \mapsto j = F(t)$.

This means that for a curve with given j-invariant, the isogenous curves (over K) correspond to the solutions $t \in K$ to the equation $F_\ell(t) = j$, of which there are at most $l + 1$.

We can thus work out *generic* ℓ-isogeny formulas once-and-for-all, and specialise in any given case.

We do also have to take account of twists (non-isomorphic curves with the same j-invariant). For simplicity we assume $j \neq 0, 1728$.

Outline of the method

Let $\ell \in \{3, 5, 7, 13\}$. Substitute $F_\ell(t)$ into a standard formula giving an elliptic curve with j-invariant j, and you get an elliptic curve E_t defined over $\mathbb{Q}(t)$ with j-invariant $j = F_\ell(t)$.

Outline of the method

Let $\ell \in \{3, 5, 7, 13\}$. Substitute $F_\ell(t)$ into a standard formula giving an elliptic curve with j-invariant j, and you get an elliptic curve E_t defined over $\mathbb{Q}(t)$ with j-invariant $j = F_\ell(t)$.

Find its ℓ-division polynomial (in $\mathbb{Q}(t)[X]$) and factor it.

Outline of the method

Let $\ell \in \{3, 5, 7, 13\}$. Substitute $F_\ell(t)$ into a standard formula giving an elliptic curve with j-invariant j, and you get an elliptic curve E_t defined over $\mathbb{Q}(t)$ with j-invariant $j = F_\ell(t)$.

Find its ℓ-division polynomial (in $\mathbb{Q}(t)[X]$) and factor it.

You will see a factor of degree $(l-1)/2$, which is the generic kernel polynomial we seek, as a polynomial in $\mathbb{Q}(t)[X]$. Specializing to $t \in K$ will give us a kernel polynomial in $K[X]$.

Outline of the method

Let $\ell \in \{3, 5, 7, 13\}$. Substitute $F_\ell(t)$ into a standard formula giving an elliptic curve with j-invariant j, and you get an elliptic curve E_t defined over $\mathbb{Q}(t)$ with j-invariant $j = F_\ell(t)$.

Find its ℓ-division polynomial (in $\mathbb{Q}(t)[X]$) and factor it.

You will see a factor of degree $(l-1)/2$, which is the generic kernel polynomial we seek, as a polynomial in $\mathbb{Q}(t)[X]$. Specializing to $t \in K$ will give us a kernel polynomial in $K[X]$.

The correct t to use are the solutions (if any) to $F_\ell(t) = j$, where $j = j(E)$.

Outline of the method

Let $\ell \in \{3, 5, 7, 13\}$. Substitute $F_\ell(t)$ into a standard formula giving an elliptic curve with j-invariant j, and you get an elliptic curve E_t defined over $\mathbb{Q}(t)$ with j-invariant $j = F_\ell(t)$.

Find its ℓ-division polynomial (in $\mathbb{Q}(t)[X]$) and factor it.

You will see a factor of degree $(l-1)/2$, which is the generic kernel polynomial we seek, as a polynomial in $\mathbb{Q}(t)[X]$. Specializing to $t \in K$ will give us a kernel polynomial in $K[X]$.

The correct t to use are the solutions (if any) to $F_\ell(t) = j$, where $j = j(E)$.

However, E_t will in general be a quadratic twist of our curve E, which we must allow for.

The case $\ell = 5$

Recall that $F_5(t) = (t^2 + 10t + 5)^3/t$. An elliptic curve with this j-invariant over $\mathbb{Q}(t)$ is

$$E_t : \qquad y^2 = x^3 - 3(j/k)x - 2(j/k)$$

where $j = F_5(t)$ and $k = j - 1728$. The 5-division polynomial of E_t has the quadratic factor

$$\Psi_t(X) = X^2 + ((2t^2+20t+10)/(t^2+4t-1))X + (t^6+42t^5+639t^4+4300t^3+120$$

To take the quadratic twist into account, we find that the kernel polynomials for the elliptic curve E with invariants c_4, c_6, j are $\Psi_t(c_4X/3c_6)$.

Larger ℓ

A similar computation gives generic kernel polynomials for ℓ-isogenies for $\ell = 7$ and $\ell = 13$. One has to do a substantial one-time factorization in $\mathbb{Q}[t, X]$, but after that the work is trivial.

Larger ℓ

A similar computation gives generic kernel polynomials for ℓ-isogenies for $\ell = 7$ and $\ell = 13$. One has to do a substantial one-time factorization in $\mathbb{Q}[t, X]$, but after that the work is trivial.

We have done similar pre-computations for all the larger ℓ which can occur as isogeny degrees over $\mathbb{Q}$: $l = 11, 17, 19, 37, 43, 67$ or 163. In each case the number of j-invariants is finite, so we no longer have a parameter t in the division polynomial, which has larger degree (up to $\frac{1}{2}(163^2 - 1) = 13284$). The one-off computation is non-trivial, but we can now compute isogenies of all degrees over $\mathbb{Q}$ very quickly without needing to risk floating-point precision issues!

Larger ℓ

A similar computation gives generic kernel polynomials for ℓ-isogenies for $\ell = 7$ and $\ell = 13$. One has to do a substantial one-time factorization in $\mathbb{Q}[t, X]$, but after that the work is trivial.

We have done similar pre-computations for all the larger ℓ which can occur as isogeny degrees over $\mathbb{Q}$: $l = 11, 17, 19, 37, 43, 67$ or 163. In each case the number of j-invariants is finite, so we no longer have a parameter t in the division polynomial, which has larger degree (up to $\frac{1}{2}(163^2 - 1) = 13284$). The one-off computation is non-trivial, but we can now compute isogenies of all degrees over $\mathbb{Q}$ very quickly without needing to risk floating-point precision issues!

Work is under way to extend this idea of "generic kernel polynomials" to larger ℓ, starting with the three cases $\ell = 11, 17, 19$ (genus 1). The implementation will work over arbitrary fields (and arbitrary characteristic).