

Mappings of elliptic curves

Benjamin Smith

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

Eindhoven, September 2008

Fields of Definition

Throughout this talk, k denotes some field.
(In practice, $k = \mathbb{F}_q$).

An object is “defined over k ” or **k -rational** if we can define or represent it using equations with coefficients in k .

We will tend to avoid characteristic 2 and 3 in our examples.

We assume you know about Elliptic Curves and their basic arithmetic.
(We will use Weierstrass models for all of our examples).

Elliptic Curves

Be careful that you understand the distinction between the elliptic curve E and the group $E(k)$ of its k -rational points.

The group law is defined for the curve E , not just the points in $E(k)$.

Example

The group law on $E : y^2 = x^3 + 1$ is defined by the “rational map”

$$(x_1, y_1) + (x_2, y_2) = (X(x_1, y_1, x_2, y_2), Y(x_1, y_1, x_2, y_2))$$

where

$$X = \frac{(x_1^2 x_2 + x_1 x_2^2 - y_1 y_2 + 2)}{(x_2 - x_1)^2}$$

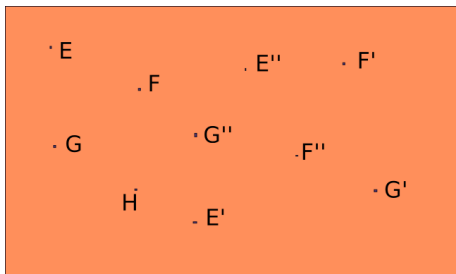
and

$$Y = \frac{(3x_1 + x_2)x_2^2 y_1 - (x_1 + 3x_2)x_1^2 y_2 - 4(y_2 - y_1)}{(x_2 - x_1)^3}.$$

Observe that $Y^2 = X^3 + 1$.

The set of all elliptic curve over k

So far this week, we've dealt with individual elliptic curves in isolation. Now we want to consider **all** the elliptic curves over k at the same time. The geometer's way of doing this is to consider the **moduli space** of elliptic curves:



Each point in the space corresponds to a class of **isomorphic** curves — that is, curves that are related by a change of coordinates.

Remark

The moduli space of elliptic curves is really a line (ie *one-dimensional*).

Polynomial maps

Now we want to start looking at **relationships** between curves.

Geometric relationships are expressed by morphisms

For projective curves, a morphism $\phi : E \rightarrow E'$ is defined by a polynomial mapping

$$\phi : (X : Y : Z) \longmapsto (\phi_0(X, Y, Z) : \phi_1(X, Y, Z) : \phi_2(X, Y, Z)),$$

where the ϕ_i are homogeneous polynomials of equal degree satisfying the defining equation of E' .

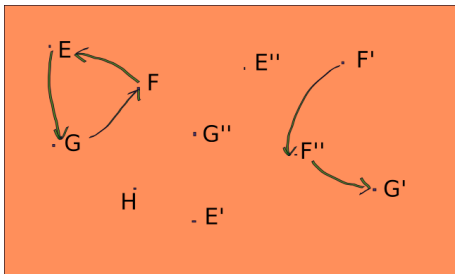
In affine coordinates, ϕ will be a **rational map** (with denominators):

$$\phi : (x, y) \longmapsto \left(\frac{\phi_0(x, y, 1)}{\phi_2(x, y, 1)}, \frac{\phi_1(x, y, 1)}{\phi_2(x, y, 1)} \right).$$

This rational map extends automatically to a polynomial map when we “complete” the curves in projective space.

Morphisms

Non-constant morphisms express algebraic relationships between curves.



- 1 Given a curve E , what does its structure tell us about the collection of morphisms from E to other curves (including E itself)?
- 2 Given a collection of morphisms $\{\phi_i : E \rightarrow E_i\}$, what do they tell us about the structure of E ?

Degree of a morphism

Every morphism of curves has an integer **degree**.

Strictly speaking, the degree of $\phi : E \rightarrow E'$ is the degree of the function field extension $k(E')/k(E)$ induced by ϕ .

We don't have time to do this properly; but note that “most of the time”, a morphism $E \rightarrow E'$ has degree n if it induces an n -to-1 mapping from $E(\bar{k})$ to $E'(\bar{k})$.

First examples

We have already met some examples of morphisms of elliptic curves:

Example

For every elliptic curve E and for every integer m , the multiplication-by- m map $[m]$ is a morphism from E to itself (an **endomorphism**).

Recall $[m]$ sends all the points in $E[m](\bar{k})$ to 0_E .

If m is not divisible by $\text{char } k$, then $E[m](\bar{k}) \cong (\mathbb{Z}/m\mathbb{Z})^2$, so $[m]$ is m^2 -to-1, and the degree of $[m]$ is m^2 .

Example

If E is defined over \mathbb{F}_q , then we also have a **Frobenius** endomorphism, denoted π_E , mapping (x, y) to (x^q, y^q) .

The degree of π_E is q .

Note that the set of fixed points of π_E is $E(\mathbb{F}_q)$.

Exercise

Why is $[m]$ a morphism? Can you represent it as a rational map?

Translations

For each point P in $E(k)$, we have a “translation” morphism $\tau_P : E \rightarrow E$ defined over k , mapping $Q \mapsto \tau(P) = Q + P$.

This is a polynomial map, since the group law is defined by polynomials.

Example

Consider the elliptic curve $E : y^2 = x^3 + 1$ over \mathbb{Q} .

If P is the point $(2, 3)$ in $E(\mathbb{Q})$, then the translation τ_P is defined by

$$\tau_P : (x, y) \mapsto \left(\frac{2((x+1)^2 - 3y)}{(x-2)^2}, \frac{3(x^3 + 6x^2 + 4 - 4(x+1)y)}{(x-2)^3} \right).$$

Homomorphisms

A homomorphism is a morphism of elliptic curves that respects the group structure of the curves.

Theorem

Every morphism $E \rightarrow E'$ is a (unique) composition of a homomorphism $E \rightarrow E'$ and a translation on E' .

Corollary

Every morphism $E \rightarrow E'$ mapping 0_E to $0_{E'}$ is automatically a homomorphism!

Warning

From now on,

we consider only morphisms sending 0_E to $0_{E'}$.

This isn't just convenient — it's also the right thing to do (in a category-theoretical sense).

Strictly speaking, an “elliptic curve defined over k ” is a pair $(E, 0_E)$, where E is a curve of genus 1 over k and 0_E is a distinguished k -rational point on E (which becomes the zero of the group law).

So morphisms $(E, 0_E) \rightarrow (E', 0_{E'})$ should map E to E' and 0_E to $0_{E'}$.

Endomorphisms

An **endomorphism** of an elliptic curve E is a homomorphism from E to itself.

The set of all endomorphisms of E is denoted $\text{End}(E)$.

The group structure on E makes $\text{End}(E)$ into a ring.

- Addition in $\text{End}(E)$ is defined by $(\phi + \psi)(P) := \phi(P) + \psi(P)$
- Multiplication in $\text{End}(E)$ is defined by $\phi\psi := \phi \circ \psi$.

$\text{End}(E)$ always contains a copy of \mathbb{Z} , in the form of the multiplication-by- m maps.

If E is defined over \mathbb{F}_q , then we also have the Frobenius endomorphism π_E .

Isomorphisms

Definition

An isomorphism is a morphism of degree 1.

(Essentially, an isomorphism is a change of coordinate system.)

Example

Consider the curve $E : y^2 + y = x^3$ over \mathbb{Q} .

There is an isomorphism $(x, y) \mapsto (2^2 3^3 x, 2^2 3^3 (2y + 1))$

from E to the Weierstrass model $E' : y^2 = x^3 + 11664$.

Twists

Note that we can have curves E and E' defined over k such that there is an isomorphism $E \rightarrow E'$ defined over \bar{k} but *not* over k .

In this case, we say that E and E' are **twists**.

Example

Consider the curves $E' : y^2 = x^3 + 11664$ and $E'' : y^2 = x^3 + 1$, both defined over \mathbb{Q} .

These curves cannot be isomorphic over \mathbb{Q} :

$E''(\mathbb{Q})$ has a point of order 2 (namely $(-1, 0)$),

while $E'(\mathbb{Q})$ has no point of order 2.

But over $\mathbb{Q}(\sqrt{2})$, we have an isomorphism $E' \rightarrow E''$ defined by $(x, y) \mapsto (2^3 3^6 \sqrt{2} \cdot x, 2^2 3^3 y)$.

We say that E' and E'' are *quadratic* twists.

The j -invariant

There exists a function

$$j : \{\text{Elliptic curves over } k\} \longrightarrow k,$$

called the **j -invariant**, such that

$$j(E) = j(E') \iff E \text{ and } E' \text{ are isomorphic over } \bar{k}.$$

In fact, j is surjective, so k is the moduli space we mentioned earlier: each value of k corresponds to a distinct \bar{k} -isomorphism class of elliptic curves defined over k .

Example

The j -invariant of $E : y^2 = x^3 + f_2x^2 + f_1x + f_0$ is

$$j(E) = \frac{-64f_2^6 + 576f_2^4f_1 - 1728f_2^2f_1^2 + 1728f_1^3}{f_2^3f_0 - \frac{1}{4}f_2^2f_1^2 - \frac{9}{2}f_2f_1f_0 + f_1^3 + \frac{27}{4}f_0^2}.$$

Remark

All the twists of E have the same j -invariant as E .

Automorphisms

An automorphism is an isomorphism from a curve to itself.

Every elliptic curve $E : y^2 = f(x)$ has two obvious automorphisms:

- 1 the trivial one, $[1] : (x, y) \mapsto (x, y)$, and
- 2 the involution $[-1] : (x, y) \mapsto (x, -y)$.

Example

The curve $y^2 = x^3 + ax$ (for any choice of $a \neq 0$) has an automorphism $(x, y) \mapsto (-x, iy)$ (where $i^2 = -1$). These curves all have j -invariant 1728.

Example

The curve $y^2 = x^3 + a$ (for any choice of $a \neq 0$) has an automorphism $(x, y) \mapsto (\zeta_3 x, y)$ (where $\zeta_3^3 = 1$). These curves all have j -invariant 0.

Remark

In these examples, the extra automorphisms may not be defined over k .

The Automorphism group

The automorphisms of E form a group, denoted $\text{Aut}(E)$. Typically, the automorphism group is as small as possible.

Theorem

Let E/k be an elliptic curve. Then $\text{Aut}(E)$ is finite, and its order is

- 2 if $j(E) \notin \{0, 1728\}$
- 4 if $j(E) = 1728$ and $\text{char } k \notin \{2, 3\}$
- 6 if $j(E) = 0$ and $\text{char } k \notin \{2, 3\}$
- 12 if $j(E) = 0 = 1728$ and $\text{char } k = 3$
- 24 if $j(E) = 0 = 1728$ and $\text{char } k = 2$.

(In the last two cases, E is always supersingular.)

Automorphisms

An automorphism is a k -automorphism if it is defined over k .

Remark

The k -automorphism group of the underlying curve of E is a semidirect product of $\text{Aut}(E)(k)$ and $E(k)$, where $E(k)$ acts by translation. This larger group is what you will get if you use `AutomorphismGroup(E)` in Magma.

Remark

The number of twists of E can be calculated by looking at the action of Galois on $\text{Aut}(E)$.

Remark

There is a slightly faster Discrete Log algorithm for curves with larger automorphism groups — see Duursma, Gaudry, and Morain (1999) for an overview.

Isogenies

Definition

An isogeny is a (geometrically surjective) homomorphism with finite kernel.

This is the definition for general abelian varieties.

For elliptic curves, we can use the equivalent and simpler

Definition (elliptic-curve specific)

An isogeny is a nonzero homomorphism.

Isogenies are determined (up to isomorphism) by their kernels:
if $\phi : E \rightarrow E'$ and $\psi : E \rightarrow E''$ are isogenies
with the same kernel, then E' and E'' are isomorphic (or twists).

Remark

Isogenies are “almost” isomorphisms.

Quotient isogenies

Given any finite subgroup S of E , we may form a quotient isogeny

$$\phi : E \longrightarrow E' = E/S$$

with kernel S using **Vélu's formulae**.

Example

Consider $E : y^2 = (x^2 + b_1x + b_0)(x - a)$.

The point $(a, 0)$ on E has order 2; the quotient of E by $\langle (a, 0) \rangle$ gives an isogeny $\phi : E \rightarrow E'$, where

$$E' : y^2 = x^3 + -(4a + 2b_1)x^2 + (b_1^2 - 4b_0)x$$

and where ϕ maps (x, y) to

$$\left(\frac{x^3 - (a - b_1)x^2 - (b_1a - b_0)x - b_0a}{x - a}, \frac{(x^2 - (2a)x - (b_1a + b_0))y}{(x - a)^2} \right).$$

Rationality of isogenies

The quotient $\phi : E \rightarrow F = E/S$ is defined over k if and only if S is defined over k (ie Galois-stable): the points of S need not be defined over k themselves.

In the case $k = \mathbb{F}_q$, the quotient ϕ is defined over \mathbb{F}_q if and only if S is fixed by Frobenius — that is, if the equations defining S are fixed by Frobenius. The elements of such an S may be defined over \mathbb{F}_{q^n} for some n , in which case they will be permuted by Frobenius.

In particular, this means that there can be isogenies from E defined over k even when the elements of their kernels are not “visible” over k .

Tate's theorem

Theorem

Let E and E' be elliptic curves over \mathbb{F}_q .

There exists an isogeny $E \rightarrow E'$ defined over \mathbb{F}_q if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.

Example

Consider $E : y^2 = x^3 - 8x + 16$ over \mathbb{F}_{101} .

We have $E(\mathbb{F}_{101}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/44\mathbb{Z}$, so $\#E(\mathbb{F}_{101}) = 88$.

The point $(5, 0)$ of E has order 2, and the quotient by $\langle(5, 0)\rangle$ is an isogeny

$$\phi : E \longrightarrow E' : y^2 = x^3 - 40x + 6.$$

Now $E'(\mathbb{F}_{101}) \cong \mathbb{Z}/88\mathbb{Z}$, so $\#E'(\mathbb{F}_{101}) = \#E(\mathbb{F}_{101})$

— but note that $E(\mathbb{F}_{101}) \not\cong E'(\mathbb{F}_{101})$.

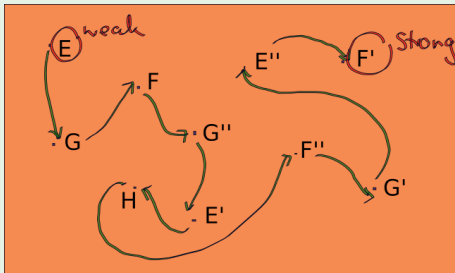
Isogenies and DLP subgroups

Isogenies induce isomorphisms on DLP subgroups
(cyclic subgroups of cryptographically interesting sizes).

We can therefore use isogenies to move DLPs between curves.

Example (may or may not be a good idea)

Teske has proposed a trapdoor system based on a hidden isogeny between a weak elliptic curve E and a “strong” elliptic curve F' :



Here E and the sequence of isogenies is given to a key escrow agency, and a DLP-based cryptosystem on F' is made public.

Splitting multiplications with isogenies

If $\phi : E \rightarrow E'$ is an isogeny such that $\phi^\dagger\phi = [m]$, then we say that “ ϕ splits multiplication-by- m ”.

When $\gcd(m, q) = 1$, what happens is that ϕ kills half the m -torsion, and the image of the remaining m -torsion is then killed by ϕ^\dagger .

Example

When ϕ has low degree and can be computed very efficiently, then computing ϕ followed by ϕ' may be faster than computing $[m]$ directly — so we can use the isogenies to speed up point multiplication (see Doche–Icart–Kohel, for example).

Frobenius isogenies

If $q = p^n$, then we have an isogeny $E \rightarrow E^p : (x, y) \mapsto (x^p, y^p)$, where E^p is the curve defined by the equation of E with all its coefficients raised to the p -th power. This is called the p -power Frobenius isogeny.

The q -power Frobenius endomorphism π_E is a composition of n successive p -power isogenies.

Theorem

Every isogeny $\phi : E \rightarrow E'$ may be expressed as a composition of isogenies with prime-order cyclic kernels and p -power Frobenius isogenies.

The characteristic polynomial of Frobenius

Let E be an elliptic curve over \mathbb{F}_q .

The Frobenius endomorphism π_E has a characteristic polynomial χ_{π_E} (a polynomial with integer coefficients such that $\chi_{\pi_E}(\pi_E) = [0]$).

We will look more closely at χ_{π_E} on Friday, but for now note that

- $\chi_{\pi_E}(X) = X^2 - t_E X + q$ for some t_E with $|t_E| \leq 2\sqrt{q}$, and
- $\chi_{\pi_E}(1) = \#E(\mathbb{F}_q)$;
- so in particular, $(q + 1) - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq (q + 1) + 2\sqrt{q}$.

The integer t_E is called the **trace** of Frobenius.

Remark

If E and E' are quadratic twists (isomorphic over \mathbb{F}_{q^2} but not over \mathbb{F}_q), then $t_{E'} = -t_E$.

Supersingular elliptic curves

Theorem

Let E be an elliptic curve over \mathbb{F}_q , where $q = p^n$. The following are equivalent:

- 1 $E[p^r] = 0$ for all $r \geq 1$
- 2 t_E is divisible by p
- 3 $\text{End}(E)$ is not commutative

If these conditions hold, we say that E is **supersingular**.

Otherwise, we say E is **ordinary**, and $E[p^r] \cong (\mathbb{Z}/p^r\mathbb{Z})$ for all $r \geq 1$.

Remark

- j -invariants of supersingular curves are isolated in the moduli space — and in fact, they are all in \mathbb{F}_{p^2} .
- It is much easier to determine $\#E(\mathbb{F}_q)$ when E is supersingular.
- If E over \mathbb{F}_q is supersingular, then the Discrete Logarithm in E is only as hard as the Discrete Logarithm in $\mathbb{F}_{q^n}^\times$ for some smallish n .