Isogenies and endomorphism rings of elliptic curves

ECC Summer School

Damien Robert

Microsoft Research

15/09/2011 (Nancy)

Outline

1. Isogenies on elliptic curves
2. Endomorphisms
3. Supersingular elliptic curves
4. Abelian varieties
5. References

Outline

1. Isogenies on elliptic curves
   - Definitions
   - Cryptographic applications of isogenies
   - Isomorphisms and twists
   - Algorithms for computing isogenies
2. Endomorphisms
3. Supersingular elliptic curves
4. Abelian varieties
5. References

Notations

- We fix a perfect field k. Since our aim is cryptographic applications of elliptic curves, most of the time k will be a finite field.
- An elliptic curve E is a smooth complete curve of genus 1 with a base point 0_E. This base point uniquely determine a structure of algebraic group on E.
- If k is a finite field, every smooth complete curve of genus 1 has a rational point, so is an elliptic curve.
- An elliptic curve $E/\mathbb{F}_q$ over a finite field of characteristic p is said to be supersingular if $\#E[p] = \{0\}$. In this case $\#E[p^n] = \{0\}$ for all n. Otherwise, $\#E[p^n] = p^n$ for all n, and E is said to be ordinary.

Complex elliptic curve

- Over $\mathbb{C}$: an elliptic curve is a torus $E = \mathbb{C}/\Lambda$, where Λ is a lattice $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, $(\tau \in \mathfrak{H})$.
- Let $\wp(z,\Lambda) = \sum_{w \in \Lambda \setminus \{0_E\}} \frac{1}{(z-w)^2} - \frac{1}{w^2}$ be the Weierstrass $\wp$-function and $E_{2k}(\Lambda) = \sum_{w \in \Lambda \setminus \{0_E\}} \frac{1}{w^{2k}}$ be the Eisenstein series of weight $2k$.
- Then $\mathbb{C}/\Lambda \to E, z \mapsto (\wp'(z,\Lambda), \wp(z,\Lambda))$ is an analytic isomorphism to the elliptic curve
$$y^2 = 4x^3 - 60E_4(\Lambda) - 140E_6(\Lambda).$$

Isogenies between elliptic curves

Definition

An isogeny is a (non trivial) algebraic map $f : E_1 \to E_2$ between two elliptic curves such that $f(P+Q) = f(P) + f(Q)$ for all geometric points $P, Q \in E_1$.

Example

- If E is an elliptic curve, the multiplication by $[m]$ is an isogeny.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic p, the Frobenius $E \to E^{(p)}, (x, y) \mapsto (x^p, y^p)$ is an isogeny.
- Let E be the elliptic curve $y^2 = x^3 + x$ over $\mathbb{F}_{17}$. Let f be the map $f(x, y) = (x, 4y)$. Is f an isogeny?

Remark

Isogenies are surjectives. In particular, if E is ordinary, any isogenous curve to E is also ordinary.

Isogenies and algebraic maps

Theorem

An algebraic map $f : E_1 \to E_2$ *is an isogeny if and only if* $f(0_{E_1}) = f(0_{E_2})$

Proof.

Over $\mathbb{C}$: a bit of work on analytic functions. □

Corollary

An algebraic map between two elliptic curves is either

- *trivial (i.e. constant)*
- *or the composition of a translation with an isogeny.*

Equivalent isogenies

- Two isogenies $f_1 : E_1 \to E_2$ and $f_2 : E_1' \to E_2'$ are equivalent if the following diagram commutes:

$$\begin{array}{ccc} E_1 & \xrightarrow{\quad f_1 \quad} & E_2 \\ \downarrow \wr & & \downarrow \wr \\ E_1' & \xrightarrow{\quad f_2 \quad} & E_2' \end{array}$$

- Let $E_1 : y^2 = x^3 + 4x + 2$ and $E_2 : y^2 = x^3 + 8x + 7$ be two elliptic curves over $\mathbb{F}_{17}$.
- Let $f_1 : E_1 \to E_1$ be the isogeny given by

$$\Big(\frac{x^9 - x^8 + 8x^7 - 2x^6 - 6x^5 + 5x^4 + x^3 - 4x^2 + 2}{x^8 - x^7 + 2x^6 - 5x^5 + 7x^4 + 4x^3 - 8x^2 + 3x - 2},$$
$$\frac{x^{12}y + 7x^{11}y + 8x^{10}y - 2x^9y + 6x^8y + 5x^7y + 8x^6y + 2x^5y + 7x^4y - 6x^3y - 7x^2y + 5xy + 4y}{x^{12} + 7x^{11} - 3x^{10} + 7x^9 - 2x^8 + 2x^7 - 4x^6 - 6x^5 - 8x^4 - 5x^3 + 3x^2 + 6x + 3}\Big)$$

  Let $f_2 : E_1 \to E_2$ be the isogeny given by

$$\Big(\frac{x^9 + 3x^7 - 5x^6 + 4x^5 - 5x^4 - 3x^3 + 6x^2 - 2x + 6}{-8x^8 + 8x^6 + 8x^5 + 4x^4 - 4x^3 - 5x^2 - 3x + 1},$$
$$\frac{x^{12}y + 3x^{10}y - 2x^9y - 5x^8y - 8x^7y - 4x^6y - x^5y - 7x^4y + x^3y - 6x^2y - 2xy - 6y}{-7x^{12} + 2x^{10} + 2x^9 - 8x^8 - 2x^7 - 8x^6 - x^5 - 5x^4 + 8x^3 - 2x^2 + 4x + 1}\Big)$$

- Is f_1 equivalent to f_2?

Equivalent isogenies

- f_1 and f_2 have the same degrees. But $E_1 \neq E_2$!
- But they have the same j-invariant ($j = 4$), so they are isomorphics.
- We could compose f_2 with an isomorphism $E_2 \xrightarrow{\sim} E_1$ and test if it is equal to f_1. But even if the curves were equal, we could still compose with automorphisms.
- So we have to construct "canonical" isogenies from f_1 and f_2.
- Easier way: compute the kernels!

$$\ker f_1 = x^4 + 8x^2 + 8x + 6$$
$$\ker f_2 = x^4 + 8x^3 + 3x^2 + 16x + 7$$

- The kernel are different, hence the isogenies are not the same. (Since $\mathrm{Aut}(E_1) = \{\pm 1\}$).
- Exercice: prove that f_1 is equivalent to the multiplication by 3.

Isogenies and kernels

Definition (Kernel)

The kernel $\ker f$ of an isogeny $f : E_1 \to E_2$ is the set of geometric points $P \in E_1$ such that $f(P) = 0_{E_2}$.

Definition (Degree)

The degree of an isogeny f is the degree of the extension field $[k(E_1) : f^* k(E_2)]$. An isogeny is separable iff $\# \ker f = \deg f$.

- The Frobenius is an inseparable isogeny of degree p.
- Every isogeny is the composition of a separable isogeny with a power of the Frobenius $\Rightarrow$ from now on we only focus on separable isogenies.

Theorem

There is a bijection between separable isogenies and finite subgroups of E:

$$(f : E_1 \to E_2) \mapsto \ker f$$
$$(E_1 \to E_1/G) \leftarrow G$$

Isogenies and multiplications

- If $H \subset G$ are finite subgroups of E, then the isogeny $E \to E/G$ splits as $E \to E/H \to (E/H)/(G/H)$.
- In particular, for every (separable) isogeny $f : E \to E'$, there exists a contragredient isogeny $f' : E' \to E$ such that $f' \circ f = [m]$, where m is the exponent of $\ker f$.
- We can also identify f' as the dual isogeny $\hat{f}$ of f (if $m = \deg f$):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \longrightarrow & E & \xrightarrow{f} & E' & \longrightarrow & 0 \\
 & & & & \downarrow\wr & & \downarrow\wr & & \\
 & & 0 & \longleftarrow & \hat{E} & \xleftarrow{\hat{f}} & \hat{E}' & \longleftarrow & \hat{K} & \longleftarrow & 0
\end{array}$$

Algorithms for manipulating isogenies

1. Given a finite subgroup $G \subset E$, construct the isogeny E/G.
2. Given E_1 and E_2, test if they are isogenous. If so construct an (or all) isogenies $E_1 \rightarrow E_2$.
3. Given E and ℓ, find ℓ-isogenous curves to E (and iterate to construct the isogeny graph).
4. Find cyclic rational subgroups of E (by using the correspondance between isogenies and kernels).

Remark

Algorithm 4 can be obtained by combining algorithms 2 and 3: first compute all ℓ-isogenous curves E', and from them compute the isogeny $E \rightarrow E'$ of degree ℓ, whose kernel give a cyclic subgroup of $E[\ell]$.

Destructive cryptographic applications

- An isogeny $f : E_1 \to E_2$ transports the DLP problem from E_1 to E_2. This can be used to attack the DLP on E_1 if there is a weak curve on its isogeny class (and an efficient way to compute an isogeny to it).

Example

- extend attacks using Weil descent [GHS02] (remember Vanessa's talk!)
- Transfert the DLP from the Jacobian of an hyperelliptic curve of genus 3 to the Jacobian of a quartic curve [Smi09].

Constructive cryptographic applications

- One can recover informations on the elliptic curve E modulo ℓ by working over the ℓ-torsion.
- But by computing isogenies, one can work over a cyclic subgroup of cardinal ℓ instead.
- Since thus a subgroup is of degree ℓ, whereas the full ℓ-torsion is of degree ℓ^2, we can work faster over it.

Example

- The SEA point counting algorithm [Sch95; Mor95; Elk97] (go to François' talk for more details).
- The CRT algorithms to compute class polynomials [Sut09; ES10].
- The CRT algorithms to compute modular polynomials [BLS09].

Further applications of isogenies

- Splitting the multiplication using isogenies can improve the arithmetic (remember Laurent's talk) [DIK06; Gau07].
- The isogeny graph of a supersingular elliptic curve can be used to construct secure hash functions [CLG09].
- Construct public key cryptosystems by hiding vulnerable curves by an isogeny (the trapdoor) [Tes06], or by encoding informations in the isogeny graph [RS06].
- Take isogenies to reduce the impact of side channel attacks [Sma03].
- Construct a normal basis of a finite field [CL09].
- Improve the discrete logarithm in $\mathbb{F}_q^*$ by finding a smoothness basis invariant by automorphisms [CL08].

Class of isomorphisms of elliptic curves

- Every elliptic curve has a Weierstrass equation:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (1)$$

with the discriminant $\Delta_E = -b_2 b_8 - 8b_3 - 27b_2 + 9b_2 b_4 b_6 \neq 0$.
(Here $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1 a_3$, $b_6 = a_3^2 + 4a_6$,
$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$).

- The j-invariant of E is

$$j_E = \frac{(b_2^2 - 24b_4)^3}{\Delta_E}$$

Theorem

Two elliptic curves E and E' are isomorphics over $\overline{k}$ if and only if $j_E = j_{E'}$.

The case of a finite field of characteristic $p > 3$

- We can always write the Weierstrass equation as

$$y^2 = x^3 + ax + b.$$

- The discriminant is $-16(4a^3 + 27b^2)$.
- The j-invariant is

$$j_E = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Isomorphisms

- The isomorphisms (over $\overline{k}$) of isomorphisms of elliptic curves in Weierstrass form are given by the maps

$$(x,y) \mapsto (u^2 x + r, u^3 y + u^2 s x + t)$$

for $u, r, s, t \in \overline{k}$, $u \neq 0$.

- If we restrict to elliptic curves of the form $y^2 = x^3 + ax + b$ then $s = t = 0$.

Proposition

Let $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ be two ordinary elliptic curves such that $j_E = j_{E'}$. Then

$E \simeq E'$ *over* $\mathbb{F}_q$

$\Leftrightarrow$ E *and* E' *are isogenous over* $\mathbb{F}_q$

$\Leftrightarrow$ $\#E = \#E'$.

Twists

- A twist of an elliptic curve $E/\mathbb{F}_q$ is an elliptic curve $E'/\mathbb{F}_q$ isomorphic to E over $\overline{\mathbb{F}}_q$ but not over $\mathbb{F}_q$.
- Every elliptic curve $E : y^2 = x^3 + ax + b$ has a quadratic twist

$$E' : \delta y^2 = x^3 + ax + b$$

  for any non square $\delta \in \mathbb{F}_q$. E and E' are isomorphic over $\mathbb{F}_q^2$.
- If $E/\mathbb{F}_q$ is an ordinary elliptic curve with $j_E \notin \{0, 1728\}$ then the only twist of E is the quadratic twist. If $j_E = 1728$, then E admits 4 twists. If $j_E = 0$, then E admits 6 twists.

When are two elliptic curves isogenous?

Theorem (Tate)

Two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if they have the same cardinal.

Proof.

- If E and E' are isogenous, they have the same cardinal: use the dual isogeny and look at the action of the Frobenius on $E[\ell]$ for ℓ not dividing the degree of the isogeny.
- The reciprocal is a theorem of Tate.

□

Isogenies between two elliptic curves

In this slide, $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ are ordinary elliptic curves over $\mathbb{F}_q$.

- If E_1 and E_2 are isogenous, then any isogeny over $\overline{\mathbb{F}}_q$ is in fact $\mathbb{F}_q$-rational.
- If $f : E_1 \to E_2$ is an isogeny over $\overline{\mathbb{F}}_q$ of prime degree, then there exist twists E_1' and E_2' of E_1 and E_2 such that f descends to an $\mathbb{F}_q$-rational isogeny $f : E_1' \to E_2'$.
- Either $\mathrm{Hom}_{\mathbb{F}_q}(E_1, E_2) = \{0\}$ or $\mathrm{Hom}_{\mathbb{F}_q}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank 2.

Computing explicit isogenies

- If E_1 and E_2 are two elliptic curves given by Weierstrass equations, a morphism of curve $f : E_1 \to E_2$ is of the form
$$f(x,y) = (R_1(x,y), R_2(x,y))$$
where R_1 and R_2 are rational functions, whose degree in y is less than 2 (using the equation of the curve E_1).
- If f is an isogeny, $f(-P) = -f(P)$. If $\operatorname{car} k > 3$ so we can assume that E_1 and E_2 are given by reduced Weierstrass forms, this mean that R_1 depends only on x, and R_2 is y time a rational function depending only on x.
- Let $w_E = dx/2y$ be the canonical differential. Then $f^* w_{E'} = c w_E$, with c in k.
- This show that f is of the form
$$f(x,y) = \left(\frac{g(x)}{h(x)}, cy \left(\frac{g(x)}{h(x)} \right)' \right).$$
$h(x)$ give (the x coordinates of the points in) the kernel of f (if we take it prime to g).
- If $c = 1$, we say that f is normalized.

Isogeny from the kernel

Remark

Every isogeny is a composition of a multiplication by $[m]$ and an isogeny with cyclic kernel (we could even further reduce to a composition with cyclic kernels of prime orders).

- Let E/k be an elliptic curve. Let $G = \langle P \rangle$ be a rational finite subgroup of E. We want to construct the isogeny $E \to E/G$.
- We need to find the Weierstrass coordinates X, Y on $k(E/G)$. But $k(E/G) = k(E)^G$ are the rational functions on E invariants under translation by a point of G.
- Moreover the Weierstrass coordinates x and y on E are characterized (up to isomorphism) by

$$\begin{aligned} v_{0_E}(x) &= -2 \qquad v_P(x) \geqslant 0 \quad \text{if } P \neq 0_E \\ v_{0_E}(y) &= -3 \qquad v_P(y) \geqslant 0 \quad \text{if } P \neq 0_E \\ y^2/x^3(0_E) &= 1 \end{aligned}$$

Vélu's formula

- Vélu constructs the isogeny $E \to E/G$ as

$$X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} (x(P+Q) - x(Q))$$
$$Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} (y(P+Q) - y(Q)).$$

  The choices are made so that the formulas give a normalized isogeny.
- Moreover by looking at the expression of X and Y in the formal group of E, Vélu recovers the equations for E/G.
- For instance if $E : y^2 = x^3 + ax + b = f(x)$ then E/G is

$$y^2 = x^3 + (a - 5t)x + b - 7w$$

  where $t = \sum_{Q \in G \setminus \{0_E\}} f'(Q)$, $u = 2 \sum_{Q \in G \setminus \{0_E\}} f(Q)$ and $w = \sum_{Q \in G \setminus \{0_E\}} x(Q) f'(Q)$.

Complexity of Vélu's formula

- Even if G is rational, the points in G may live to an extension of degree up to $\#G-1$.
- Thus summing over the points in the kernel G can be expensive.
- Let $h(x)=\prod_{Q\in G\backslash\{0_E\}}(x-x(Q))$. The symmetry of X and Y allows us to express everything in term of h.
- For instance is E is given by a reduced Weierstrass equation $y^2=f(x)$, we have

$$f(x,y)=\left(\frac{g(x)}{h(x)}, y\left(\frac{g(x)}{h(x)}\right)'\right), \text{ with}$$

$$\frac{g(x)}{h(x)}=\#G.x-\sigma-f'(x)\frac{h'(x)}{h(x)}-2f(x)\left(\frac{h'(x)}{h(x)}\right)',$$

where σ is the first power sum of h (i.e. the sum of the x-coordinates of the points in the kernel).
- When $\#G$ is odd, $h(x)$ is a square, so we can replace it by its square root.
- The complexity of computing the isogeny is then $O(M(\#G))$ operations in k.

Computing isogenous curves from E

- Let E be an elliptic curve and ℓ a prime number. We want to compute all ℓ-isogenous elliptic curves to E.
- Easy! Compute the rational cyclic subgroups of $E[\ell]$ and apply Vélu's formulas. These subgroups can be obtained as factors of the ℓ-division polynomial $\prod_{Q \in E[\ell] \setminus \{0_E\}} (x - x(Q))$.
- But the division polynomial has degree $(\ell^2 - 1)/2$ (if ℓ odd), and factorizing it will cost $O(\ell^{3.63})$. We only want to compute isogenies of degree ℓ. Can we do better?

Modular polynomials

Here $k = \overline{k}$.

Definition (Modular polynomial)

The modular polynomial $\varphi_\ell(x,y) \in \mathbb{Z}[x,y]$ is a bivariate polynomial such that $\varphi_\ell(x,y) = 0 \Leftrightarrow x = j(E)$ and $y = j(E')$ with E and E' ℓ-isogeneous.

- Roots of $\varphi_\ell(j(E),.) \Leftrightarrow$ elliptic curves ℓ-isogeneous to E. There are $\ell + 1 = \#\mathbb{P}^1(\mathbb{F}_\ell)$ such roots if ℓ is prime.
- φ_ℓ is symmetric.
- The height of φ_ℓ grows as $O(\ell)$.

Rational roots of the modular polynomials

Theorem

- *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with j-invariant not equal to* 0 *or* 1728*.*
- *Let ℓ be prime and j' be a root of $\varphi_\ell(j_E, \cdot)$ over $\mathbb{F}_{q^n}$.*
- *Then j' corresponds to a $\mathbb{F}_{q^n}$-rational ℓ-isogeny $E \to E'$.*

Proof.

There exist a $\overline{\mathbb{F}}_q$-isogeny between E and E' so a $\mathbb{F}_{q^n}$-isogeny on twists of E and E'. But with the hypothesis, the only twist of E is the quadratic one, so by applying a quadratic twist to the isogeny, we find a $\mathbb{F}_{q^n}$-rational isogeny starting from E. □

Corollary

We can use the modular polynomial φ_ℓ to construct ℓ-isogeny graphs!

Computing the modular polynomial

1. The complex analytic method: if we see $\tau \mapsto j(\tau)$ and $\tau \mapsto j(\tau/\ell)$ as a modular functions on $\mathfrak{H}$; then $\varphi_\ell(\cdot, j)$ is the minimal polynomial of $j(\cdot/\ell)$ in $\mathbb{C}(j)$. One can then recover the polynomial by computing the Fourrier coefficients of j and $j(\cdot/\ell)$ with high precision.
2. The CRT method: use Vélu's formulas to compute $\varphi_\ell \mod p$ for small p and the CRT to recover the full modular polynomial.

Remark

- *Using asymptotically fast algorithms, both algorithms are quasilinear in the size ℓ^3 of φ_ℓ, so the computations are memory bounded. But the CRT algorithm allow to compute the specialization $\varphi_\ell(j, \cdot) \in \mathbb{F}_p[x]$ directly and is the faster in practice.*
- *To reduce the size of the coefficients, one use a different modular function in $X_0^*(\ell)$ than $j(\tau/\ell)$.*

Finding an isogeny between two isogenous elliptic curves

- Let E and E' be ℓ-isogenous abelian varieties (we can check that $\varphi_\ell(j_E, j_{E'}) = 0$. We want to compute the isogeny $f : E \to E'$.
- The explicit forms of isogenies are given by Vélu's formula, which give normalized isogenies. We first need to normalize E'.
- Over $\mathbb{C}$, the equation of the normalized curve E' is given by the Eisenstein series $E_4(\ell\tau)$ and $E_6(\ell\tau)$. We have $j'(\ell\tau)/j(\ell\tau) = -E_6(\tau)/E_4(\tau)$. By differencing the modular polynomial, we recover the differential logarithms.
- We obtain that from $E : y^2 = x^3 + ax + b$, a normalized model of $j_{E'}$ is given by the Weierstrass equation

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

where $A = -\frac{1}{48}\frac{J^2}{j_{E'}(j_{E'}-1728)}$, $B = -\frac{1}{864}\frac{J^3}{j_{E'}^2(j_{E'}-1728)}$ and $J = -\frac{18}{\ell}\frac{b}{a}\frac{\varphi_\ell'^{(X)}(j_E, j_{E'})}{\varphi_\ell'^{(Y)}(j_E, j_{E'})} j_E$.

Remark

$E_2(\tau)$ is the differential logarithm of the discriminant. Similar methods allow to recover $E_2(\ell\tau)$, and from it $\sigma = \sum_{P \in K \setminus \{0_E\}} x(K)$.

Finding the isogeny between the normalized models (I: Stark's method)

- We need to find the rational function $I(x) = g(x)/h(x)$ giving the isogeny $f : (x, y) \mapsto (I(x), yI'(x))$ between E and E'.
- Over $\mathbb{C}$ the coordinates of the elliptic curve are given by the elliptic functions: $x = \wp(z)$ and $y = \wp'(z)$.
- We have to find I such that $\wp_{E'}(z) = I \circ \wp_E(z)$.
- Stark's idea is to develop $\wp_{E'}$ as a continuous fraction in $\wp_E$, and approximate I as p_n/q_n.
- This algorithm is quasi-quadratic ($\widetilde{O}(\ell^2)$).

Finding the isogeny between the normalized models (II: Elkie's method)

- We need to find the rational function $I(x) = g(x)/h(x)$ giving the isogeny $f : (x,y) \mapsto (I(x), yI'(x))$ between E and E'.
- Plugging f into the equation of E' shows that I satisfy the differential equation

$$(x^3 + ax + b)I'(x)^2 = I(x)^3 + AI(x) + B.$$

- Using an asymptotically fast algorithm to solve this equation yields $I(x)$ in time quasi-linear ($\widetilde{O}(\ell)$).
- Knowing σ gains a logarithmic factor.

Finding an isogeny between two isogenous elliptic curves (the case of small characteristic)

- The preceding algorithm needs $p > 8\ell - 5$ to solve the differential equation.
- Idea in small characteristic: lift the curves to $\mathbb{Q}_q$ by taking lifts $\widetilde{j}_E$ and $\widetilde{j}_{E'}$ such that $\varphi_\ell(\widetilde{j}_E, \widetilde{j}_{E'}) = 0$ and apply the preceding algorithm.
- Even if E' is normalized, we need the modular polynomial to lift E' and normalize the lift.

Finding an isogeny: total complexity

To summarize, we have the following algorithm to find an isogeny from E in large characteristic:

Algorithm ([BMS+08])

1. *Compute φ_ℓ (cost $\widetilde{O}(\ell^3)$)*
2. *Specialize on j_E to obtain $\varphi_\ell(X, j_E)$ (cost $\widetilde{O}(\ell^2 \log q)$)*
3. *Find a root $j_{E'}$ of $\varphi_\ell(X, j_E)$ to obtain the j-invariant of a ℓ-isogenous curve E' (cost $\widetilde{O}(\ell \log^2 q)$).*
4. *Compute the normalized model for E' (cost $\widetilde{O}(\ell^2 \log q)$).*
5. *Solve the differential equation (cost $\widetilde{O}(\ell \log q)$).*

Finding an isogeny: total complexity

With the adaptation in small characteristic still of total cost $\widetilde{O}(\ell^3 + \ell \log^2 q)$:

Algorithm ([LS08])

1. *Compute* $\varphi_\ell(X, j_E)$ (cost $\widetilde{O}(\ell^3 + \ell^2 \log q)$).
2. *Lift* j_E *and find a root* $\widetilde{j}_{E'}$ *in precision* $O(1 + \log^2 \ell / \log q)$ (cost $\widetilde{O}(\ell \log^2 q)$).
3. *Compute the normalized model for* $\widetilde{E}'$ (cost $\widetilde{O}(\ell^2 \log q)$).
4. *Solve the differential equation in* $\mathbb{Q}_q$ (cost $\widetilde{O}(\ell \log q)$).
5. *Reduce in* $\mathbb{F}_q$ (cost $\widetilde{O}(\ell \log q)$).

Finding an isogeny between two isogenous elliptic curves (the case of small characteristic): Couveigne's algorithm

Another idea to compute the isogeny in the ordinary case comes from Couveigne:

Algorithm

1. *Find generators P and P' of the cyclic groups $E[p^\alpha]$ and $E'[p^\alpha]$ for $p^\alpha << \ell$.*
2. *Interpolate the algebraic map $f : E[p^\alpha] \to E'[p^\alpha], iP \mapsto iP'$.*
3. *Test if f is an isogeny.*

- [Cou94] works with formal groups.
- [Cou96] use p-descent and towers of Artin-Schreier extensions. The best implementation [Feo10a] has complexity $\widetilde{O}(\ell^2)$.
- But the complexity is exponential in $\log(p)$.

Other algorithms to compute the isogeny

- Lercier for $p = 2$: solve the differential equation using linear algebra. Cost $\widetilde{O}(\ell^3 \log q)$ operations, in practice the fastest for $p = 2$.
- Joux and Lercier: lift in $\mathbb{Q}_q$ with precision $O(\ell)$. Cost $\widetilde{O}(\ell^2(1+\ell/p)\log q)$; useful for the intermediate case $p \approx \log q$.
- When the degree ℓ is not known but only bounded by L. The naive method is to apply one of the above algorithm for all $\ell \leq L$. This increase the cost by a degree 1 in L. However, Couveigne's algorithm can be adapted to stay in $\widetilde{O}(L^2)$ [Feo10b].
- Subexponential algorithms for computing isogenies of large degree [JS10; CJS10].

Outline

1 Isogenies on elliptic curves

2 Endomorphisms
- Definition
- The type of endomorphism rings
- Endomorphisms and isogenies
- Computing the endomorphism ring and applications

3 Supersingular elliptic curves

4 Abelian varieties

5 References

The characteristic polynomial of the Frobenius

From now on k will represent a finite field: $k = \mathbb{F}_q$.

- There exist a unique polynomial χ_π such that for every n prime to the characteristic p, $\chi_\pi \mod n$ is the characteristic polynomial of the action of the Frobenius π on $E[n]$ (here $\pi = \mathrm{Fr}_{\mathbb{F}_q}$).
- We have $\chi_\pi(\pi) = 0$, and $\#E = \chi_\pi(1)$.
- We have $\chi_\pi = X^2 - tX + q$ where the trace t is such that $|t| \leqslant 2\sqrt{q}$ (Hasse).

The endomorphism ring

Definition

- If E_1 and E_2 are elliptic curves, we note $\mathrm{Hom}_k(E_1, E_2)$ the $\mathbb{Z}$-module of all k-morphisms from E_1 to E_2. The endomorphism ring $\mathrm{End}_k(E)$ is then $\mathrm{End}_k(E) = \mathrm{Hom}_k(E, E)$.
- We note $\mathrm{End}_k^0(E) = \mathrm{End}_k(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ the endomorphism fraction ring.

Remark

- *Every non nul element of* $\mathrm{Hom}_k(E_1, E_2)$ *is an isogeny (possibly non separable).*
- $\mathrm{End}_k^0(E_1)$ *is a division algebra, and* $\mathrm{End}_k(E_1)$ *is an order in it.*
- *If* $\mathrm{Hom}_k(E_1, E_2) \neq 0$, *then* $\mathrm{End}_k^0(E_1) = \mathrm{End}_k^0(E_2)$ *and* $\mathrm{Hom}_k(E_1, E_2)$ *is a free* $\mathbb{Z}$*-module of the same rank as* $\mathrm{End}_k(E_1)$.
- *If* $\mathcal{E}$ *is the isogeny class of* E, $\mathrm{End}_k^0(E)$ *does not depend on the curve* $E \in \mathcal{E}$.
- $\mathrm{End}_k(E)$ *is either commutative of rank* 2, *or an order of rank* 4 *in a quaternion algebra.*

The ordinary case

If E is ordinary, then

- χ_π is irreducible.
- $K = \mathrm{End}_k^0(E)$ is a quadratic imaginary field.
- K is generated by π: $K = \mathbb{Q}(\pi)$.
- $\mathrm{End}_k(E)$ is an order O in K.
- For any extension k' of k we have $\mathrm{End}_k(E) = \mathrm{End}_{k'}(E) = \mathrm{End}_{\overline{k}}(E)$.

Remark

If k' is an extension of k of degree n, then the Frobenius of $E_{k'}$ seen in K is π^n.

From now on, we assume that E is ordinary, and we note $O = \mathrm{End}_k(E)$ and K the quadratic imaginary field $\mathrm{End}_k^0(E)$.

Automorphisms and twist

- The automorphisms of E are the inversible elements in $O = \operatorname{End} E$.
- All inversible elements are roots of unity.
- We usually have $O^* = \{\pm 1\}$ except in the following exceptions:
  1. $j_E = 1728$ ($p \neq 2, 3$), in this case O is the maximal order in $\mathbb{Q}(i)$ and $\#O^* = 4$;
  2. $j_E = 0$ ($p \neq 2, 3$), in this case O is the maximal order in $\mathbb{Q}(i\sqrt{3})$ and $\#O^* = 6$;
  3. $j_E = 0$ ($p = 3$), in this case E is supersingular and $\#O^* = 12$;
  4. $j_E = 0$ ($p = 2$), in this case E is supersingular and $\#O^* = 24$.
- The Frobenius $\pi \in K$ characterizes the isogeny class of E (Tate). A twisted isogeny class will correspond to a Frobenius $\pi' \neq \pi$, where there exist n with $\pi^n = \pi'^n$. This give a bijection between the twisted isogeny class and the roots of unity in K.
- More generally, there is a bijection between O^* and the twists of E.

Reduction and lifting (see Marco's talk)

- Let O be an order in a imaginary quadratic field K. Then they are h_O (the class number of O) elliptic curves over $\overline{\mathbb{Q}}$ with endomorphism ring O. They are defined over the ray class field H_O of O.
- If $p \nmid \Delta_O$, p is a prime of good reduction. Let $\mathfrak{p}$ be a prime above p in H_O. If p is inert in K, $E_{\mathfrak{p}}$ is supersingular. If p splits, $E_{\mathfrak{p}}$ is ordinary, and its endomorphism ring is the minimal order containing O of index prime to p.
- Reciprocally, if $E/\mathbb{F}_q$ is an ordinary elliptic curve, the couple $(E, \mathrm{End}(E))$ can be lifted over $\mathbb{Q}_q$.

Corollary

- *If $E/\mathbb{F}_q$ is an ordinary elliptic curve, then* $\mathrm{End}(E)$ *is an order in* $K = \mathbb{Q}(\pi)$ *of conductor prime to* p*. For every order* O *of* K *such that* $\mathbb{Z}[\pi] \subset O$*, there exist an isogenous curve whose endomorphism ring is* O*.*
- *Reciprocally, for every order* O *of discriminant a non zero square modulo* p*; let* n *be the order of one of the prime above* p *in the class group of* O*. Then there exist an (ordinary) elliptic curve* E' *over* $\mathbb{F}_{q^n}$ *with* $\mathrm{End}(E') = O$*.*

The structure of the rational points

Theorem (Lenstra)

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve. We have as $\mathrm{End}_{\mathbb{F}_q}(E)$-modules

$$E(\mathbb{F}_{q^n}) \simeq \frac{\mathrm{End}_{\mathbb{F}_q}(E)}{\pi^n - 1}$$

Corollary

- *Let $a, m \in \mathbb{Z}$ be such that $O_K = \mathbb{Z}[\frac{\pi - a}{m}]$.*
- *Let γ_E be the index of O in O_K.*
- *Then $E(\mathbb{F}_q) = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$ where $n_1 \mid n_2$ and $n_1 n_2 = \#E(\mathbb{F}_q)$.*
- *Explicitly, we have: $n_1 = \gcd(a - 1, m/\gamma_E)$.*

- Exercice: show that $n_1 \mid q - 1$ (use the Weil pairing).

Endomorphisms and isogenies

- Let $f : E_1 \to E_2$ be an isogeny of degree ℓ prime. Then either
  1. f is an ascending isogeny: $O_1 \subset O_2$ with $[O_2 : O_1] = \ell$;
  2. f is a descending isogeny: $O_2 \subset O_1$ with $[O_1 : O_2] = \ell$;
  3. f is an horizontal isogeny: $O_1 = O_2$.
- The horizontal case can only happen when O_1 is maximal locally in ℓ: $(O_1)_\ell = (O_K)_\ell$.
- Let $\ker f$ be the kernel of f. Let $O_f \subset O_1$ be the subring (of index ℓ) of isogenies fixing $\ker f$. Then f induce an injection $O_f \hookrightarrow O_2$.
- If $\psi \in O_1^*$ is an automorphism, then either ψ fixes $\ker f$ and descends to an automorphism of O_2, or ψ induce an isogeny equivalent to f.

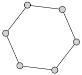
Isogeny graph: the local picture

- Let E be an ordinary elliptic curve with endomorphism ring O, and $\ell \neq p$ be a prime.
- We note Δ the discriminant of O_K, and $\Delta_\pi = t^2 - 4p$ the discriminant of χ_π.
- We have $\Delta_\pi = \gamma^2 \Delta$, where γ is the conductor of $\mathbb{Z}[\pi] \subset O_K$.
- We note ν the ℓ-adic valuation of γ, and ν_E the ℓ-adic valuation of the conductor γ_E of $O \subset O_K$.

Isogeny graph: horizontal isogenies

If $\nu = 0$, then every ℓ-isogeny is horizontal, and there are $1 + \frac{\Delta}{\ell}$ such isogeny. More precisely:

1. If ℓ splits in O. In this case Δ_π is a non zero square mod ℓ, and the Frobenius acts on $E[\ell]$ as $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ where the two eigenvalues λ and μ are distinct. The modular polynomial splits into irreducible factors of degree $1, 1, r, \ldots, r$ where r is the order of $\lambda/\mu \in \mathbb{F}_\ell$. There are 2 horizontal isogenies.



2. If ℓ is inert in O. Then Δ_π is not a square modulo ℓ. The two eigenvalues λ and μ are conjugate in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$. The modular polynomial splits as irreducible factors of degree r, where r is the smallest number such that $\lambda^r \in \mathbb{F}_\ell$ (or equivalently such that π^r acts like a scalar on $E[\ell]$). There are no horizontal isogenies.

3. If ℓ is ramified in O. Then $\Delta_\pi \equiv 0 \mod \ell$. In this case π acts on $E[\ell]$ as $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. The modular polynomial splits into two irreducible factors of degree 1 and ℓ. There is one horizontal isogeny.

Isogeny graph: vertical isogenies

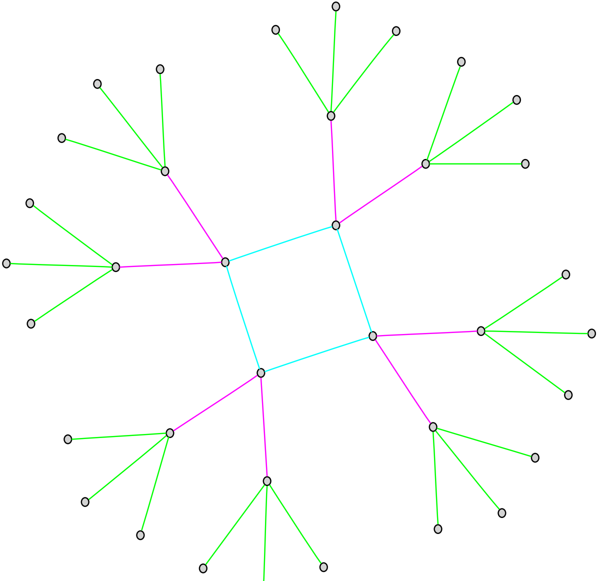
If $\nu \neq 0$. Then

- If $\nu_E = 0$, that is if $O_\ell = (O_K)_\ell$. There are $1 + \frac{\Delta}{\ell}$ horizontal isogenies, and $\ell - \frac{\Delta}{\ell}$ descending isogenies (that is $\ell - 1$, $\ell + 1$ or ℓ whether ℓ splits, is inert or is ramified in O_K).
- If $0 < \nu_E < \nu$, there is one ascending isogeny, and ℓ-descending ones.
- If $\nu_E = \nu$, that is $O_\ell = \mathbb{Z}[\pi]_\ell$, there is only one ascending isogeny.

In the first two cases, π acts as a scalar on $E[\ell]$ (and the modular polynomial splits completely), while in the last case π acts as $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ (and the modular polynomial splits into two irreducible factors of degree 1 and ℓ).

Isogeny graph: graphic interpretation of the local picture

The isogeny graph looks like a volcano [FM02]:

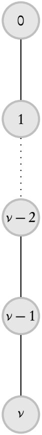


Isogeny graph: graphic interpretation of the local picture

- The volcano has height ν.
- The crater has length:
  1. 0 if ℓ is inert;
  2. 1 if ℓ splits;
  3. the order of $\mathfrak{l}$ in the class group of the order of the curves in the crater when ℓ splits as $\mathfrak{l}\bar{\mathfrak{l}}$.
- Taking an extension only increase the height of the volcano;
- If the height ν is non 0, then the only extension increasing the height are of degrees d with $\ell \mid d$.
- If $d = \ell$ the height increase only by one (except possibly when $\ell = 2$ and $\nu = 1$).

The structure of the ℓ^∞-torsion in the volcano

- If E is on the floor, then $E[\ell^\infty](\mathbb{F}_q)$ is cyclic: $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^m\mathbb{Z}$ (possibly $m = 0$).
- If E is on level $\alpha < m/2$ above the floor, then $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^\alpha \oplus \mathbb{Z}/\ell^{m-\alpha}$.
- If E is on level $\alpha \geq m/2$, then m is even and $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{m/2} \oplus \mathbb{Z}/\ell^{m/2}$.



$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{m/2}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m/2}\mathbb{Z}$

$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{m/2}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m/2}\mathbb{Z}$

$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{2}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m-2}\mathbb{Z}$

$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell^{m-1}\mathbb{Z}$

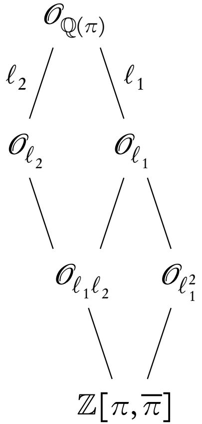
$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{m}\mathbb{Z}$

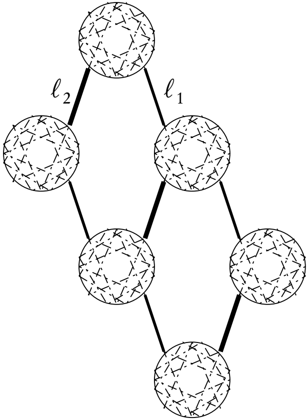
The global structure

Theorem (Complex multiplication)

Let E be an elliptic curve with endomorphism ring O. Then the set of horizontal isogenies form a principal homogeneous space under the class group of O.

This yield the following global picture (courtesy of Gaetan Bisson):





Finding the endomorphism ring

- Locally: for each $\ell \mid \gamma$, follow 3 paths in the ℓ-volcano. The first path reaching the floor give us the height of the curve in the volcano.
  Since $\gamma \approx \sqrt{q}$, this is exponential.
- Globally, by using relations in the class groups of the orders. If R is a relation in $\mathrm{Cl}(O)$ but the corresponding isogeny path is not cyclic then we know that $O \not\subset \mathrm{End}(E)$. This give a subexponential algorithm (under GRH). More details will be given in Gaetan's talk next week.

Cryptographic applications of the endomorphism ring

- It is a finer grained invariant than the number of point.
- It gives an idea of "where we are" in the full isogeny graph.
- It is used by the CRT method to compute class polynomials: from a curve in the isogeny class, we want to find a curve with maximal endomorphism ring.
- The cycle in the crater can be used to compute $\chi_\pi \mod \ell^n$.

Outline

1 Isogenies on elliptic curves

2 Endomorphisms

3 Supersingular elliptic curves

4 Abelian varieties

5 References

Isogeny class of supersingular curves

Let $q = p^n$. The isogeny classes of elliptic curves are given by the value of the trace t by Tate's theorem. The possible value of t are:

- t prime to p, in this case the isogeny class is ordinary.
- The other cases give supersingular elliptic curves. The endomorphism fraction ring $\mathrm{End}^0_k(\mathscr{E})$ of the isogeny class is either a quaternion algebra of rank 4, or an imaginary quadratic field. In the latter case, it will become maximal after an extension of degree d, with:
  1. If n is even:
     - $t = \pm 2\sqrt{q}$, this is the only case where $\mathrm{End}^0_k(\mathscr{E})$ is a quaternion algebra.
     - $t = \pm\sqrt{q}$ when $p \not\equiv 1 \mod 3$, here $d = 3$.
     - $t = 0$ when $p \not\equiv 1 \mod 4$, here $d = 2$.
  2. If n is odd:
     - $t = 0$, here $d = 2$.
     - $t = \pm\sqrt{2q}$ when $p = 2$, here $d = 4$.
     - $t = \pm\sqrt{3q}$ when $p = 3$, here $d = 6$.

The commutative case

- If $K = \mathrm{End}^0_k(E)$ is commutative, then χ_π is irreducible and $K = \mathbb{Q}(\pi)$. $\mathbb{Z}[\pi]$ is maximal for every $\ell \neq \{2, p\}$.
- The endomorphism rings of the isogeny class are the orders containing $\mathbb{Z}[\pi]$ maximal at p.
- If O is such an order, the class group $\mathrm{Cl}(O)$ acts principally on the set of elliptic curves in the isogeny class with O as ring of endomorphisms.
- If k' is such that $\mathrm{End}^0_{k'}(E)$ is maximal (i.e. a quaternion algebra), then it can happen that some curves E' in the isogeny class become isomorphic to E over k'.

The maximal case

- If $K = \mathrm{End}_k^0(E)$ is non commutative, then it is the quaternion algebra ramified only at p and ∞. The frobenius $\pi = p^{m/2} \in \mathbb{Z}$ and χ_π is a square. The endomorphism rings in the isogeny class corresponds to the maximal orders of K.
- If O is any maximal order of K, then the isogeny class of E (up to isomorphism) is of size $\# \mathrm{Cl}(O)$. There is one or two curve in the isogeny class with endomorphism ring O, according to whether $\mathfrak{p}$ is principal or not, where $\mathfrak{p}$ is the ideal such that $\mathfrak{p}^2 = p$.
- If n is even there are two isogeny classes (quadratic twists of each other) with a maximal endomorphism ring.

Remark

Any two supersingular elliptic curves become isogenous after a quadratic extension of degree $2d$ (with d the degree where their endomorphism ring become maximal). But a new maximal class and up to 3 commutative classes appear in this extension.

Supersingular elliptic curves over $\overline{\mathbb{F}}_p$

- In characteristic p, every supersingular curve is defined over $\mathbb{F}_{p^2}$.
- For every $\ell \neq p$, the isogeny graph of supersingular curves (up to twists) over $\mathbb{F}_{p^2}$ is connected. It has $p/12 + O(1)$ vertices, and diameter $O(\log p)$.
- The absolute endomorphism ring $\mathrm{End}_{\overline{k}}(E)$ of a supersingular curve is a maximal order in the quaternion algebra ramified only at p and ∞.
- There is a bijection between the set of such orders, and the set of supersingular elliptic curve (up to an action of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$).

Outline

1 Isogenies on elliptic curves

2 Endomorphisms

3 Supersingular elliptic curves

4 Abelian varieties

5 References

Abelian varieties

Definition

- An Abelian variety is a complete connected group variety over a base field k. The group law is abelian.
- A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

Example

- Abelian varieties of dimension 1 are elliptic curves.
- The Jacobian of a curve of genus g is an abelian variety of dimension g.

Non absolutely simple abelian varieties

Definition

- An abelian variety A_k is simple if the only subvariety of A_k are 0_{A_k} and itself.
- A_k is absolutely simple if it is simple over $\overline{k}$.

Even if an abelian variety A is ordinary, lot of funny things can happen if it is not absolutely simple:

- Not every non zero morphism is an isogeny.
- The endomorphism ring $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ may not be a division algebra.
- We can have $\mathrm{End}^0_{k'}(A) \neq \mathrm{End}^0_k(A)$ for extensions k' of k.
- A can be isogenous to another abelian variety A', isomorphic to it over an extension of k, but not isomorphic to it over k.

Decomposing abelian varieties

Theorem (Poincaré-Weil)

Every abelian variety A is isogenous to a product of simple abelian varieties $A = \prod A_i^{m_i}$. The decomposition is entirely determined by χ_{π_A}.

- $\mathrm{End}^0(A_i)$ is a division algebra.
- $\mathrm{End}^0(A) = \prod M_{m_i}(\mathrm{End}^0(A_i))$.

Theorem (Tate)

$Hom_k(A, B)$ is free of rank the number of common roots (with multiplicity) of χ_{π_A} and χ_{π_B}.

Endomorphism rings of abelian varieties

Let A be a simple abelian variety of dimension g. Then

1. $\chi_\pi = m_A^e$ where m_A is the minimal polynomial of the Frobenius and is irreducible.
2. $\mathrm{End}^0(E)$ is a division algebra of center $\mathbb{Q}(\pi)$. The type of $\mathrm{End}^0(E)$ is entirely determined by π.
3. We have $2g = de$, where d is the degree of m_A. $\mathrm{End}^0(E)$ is of rank de^2.

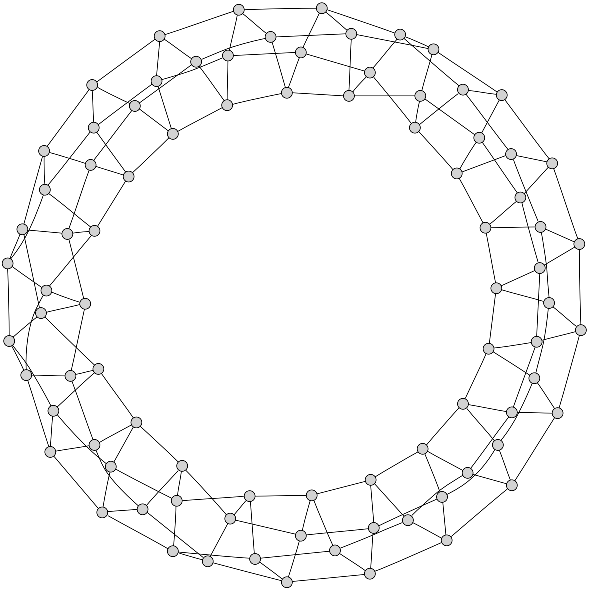
Remark

- *If A is ordinary, then $e = 1$, χ_π is irreducible and $K = \mathrm{End}_k^0(E)$ is a CM-field of rank $2g$.*
- *Moreover if A is absolutely simple, then $K = \mathbb{Q}(\pi) = \mathbb{Q}(\pi^n)$ for every n and* $\mathrm{End}_k(A) = \mathrm{End}_{\overline{k}}(A)$.

Computing isogenies and endomorphisms

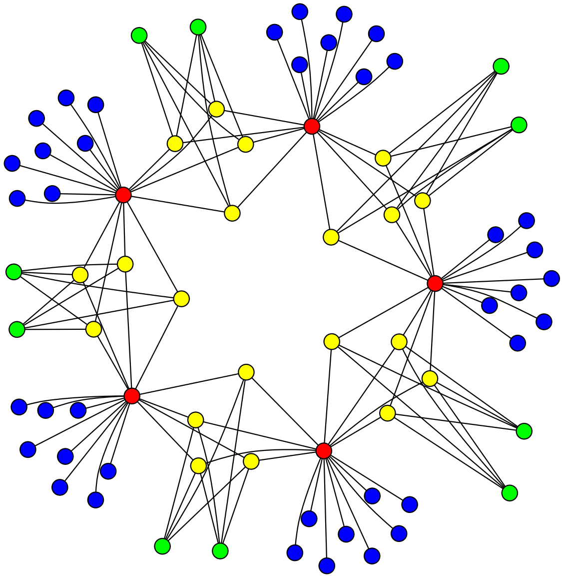
- In dimension 2, one can define modular polynomials using the Igusa invariants [Gau00; Dup06; BL09]. But these are too big to compute even for $\ell \geqslant 3$.
- We have an equivalent of Vélu's formula for maximally isotropic kernels [LR10; CR11].
- We also have subexponentials algorithms to compute the endomorphism ring in dimension 2 [Bis11b].
- See the package AVIsogenies [BCR10] for an implementation of isogenies and endomorphism ring computation (mostly restricted to dimension 2 for now).

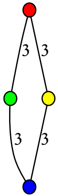
Isogeny graph in genus 2: example of horizontal isogenies



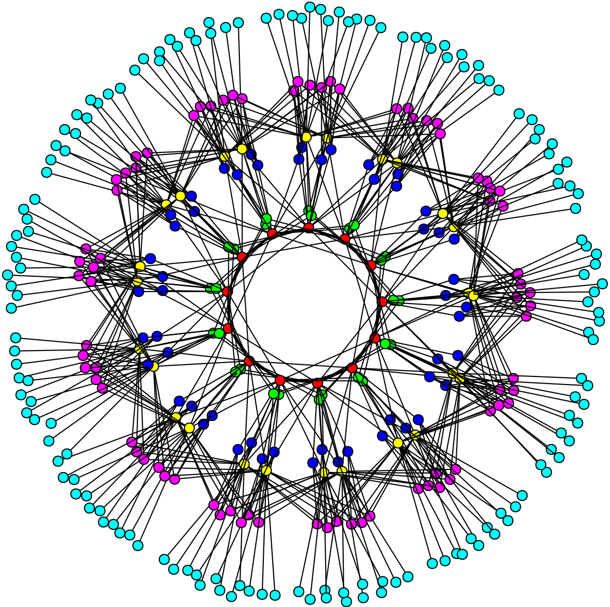
Isogeny graph in genus 2: vertical isogenies

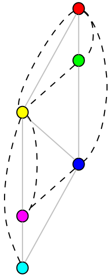
Computations done by Gaetan Bisson using AVIsogenies.





Isogeny graph in genus 2: vertical isogenies





Outline

1 Isogenies on elliptic curves

2 Endomorphisms

3 Supersingular elliptic curves

4 Abelian varieties

5 References

Elliptic curves

- For a meta look at attacks on elliptic curves using isogenies to transfert the DLP: [KKM09, Section 11.2].
- Computing the modular polynomial: [Eng09a; BLS09].
- Different methods to compute class fields polynomials (the best known methods use the CRT and isogenies): [Eng09b; Sut09; ES10].
- Explicit isogenies in large characteristic: see [Elk92; Elk97]; and [BMS+08] for the best current known algorithm, with a nice history of previous methods.
- Explicit isogenies in small characteristic: [JL06; LS08] for methods based on lifting, [Cou94; Cou96] for Couveigne's algorithm. The current best implementation of Couveigne's algorithm is in [Feo10a], a nice summary is in [Feo10b].
- Some papers on SEA point counting algorithm [Sch95; Mor95; Elk97; Ler97].
- About isogenies and isomorphisms descending to the base field, see [Cox89, Proposition 14.19] and [Sch95, Proposition 6.1].
- See [Sil86, Chapter X, Theorem 2.2] for the equivalence between automorphisms and twists.
- An algorithm to compute endomorphism ring was developed in Kohel's thesis [Koh96]. Some extensions to supersingular curves are in [ML04; Cer04].
- Developing the result of Kohel's led to the notion of "isogeny volcano" [FM02] and improvements of the computation of the endomorphism ring [Fou01] with applications to the CRT method to compute class polynomials.
- Finally, a subexponential algorithm is developped in [BS09; Bis11a; Bis11b].
- One can also use the cycle given by the crater of the volcano to recover the trace of the Frobenius modulo a power of ℓ [CM94; CDM96; FM02; Fou01].

- Using pairings to go up in the Volcano [IJ10]. The ℓ^∞-torsion in the volcano is described there, and also in [MMS+06].

Abelian varieties

- For an introduction to abelian variety, see [Mil91]. For more informations, see [Mum70], with [Mil85; Mil86] for simplified proofs using étale cohomology, and [GM07] for a more recent account. For abelian varieties over $\mathbb{C}$, see [Mum83; Mum84; Mum91] and a more recent account in [BL04].
- Some nice informations on abelian varieties over finite fields (Tate's theorem, Honda-Tate theory) see [WM71] and [Wat69] for a more complete treatment.
- A description of ordinary abelian variety over a finite field is given by an equivalence of category [Del69], the link is further studied in [How95].
- For algebraic theta functions, see [Mum66; Mum67a; Mum67b], and some new results in [Kem89].
- Computing modular polynomials in genus 2: [Gau00; Dup06; BL09]. Computing a certain modular correspondance using theta functions [FLR11].
- Computing isogenies in abelian varieties using theta functions [LR10; CR11].
- For an introduction to the use of theta functions in cryptography (arithmetic, pairings, isogenies) see [Rob10].
- Computing endomorphism ring see [EL07; FL08; Wag09; Bis11b].

Bibliography

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*. Second. Vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Berlin: Springer-Verlag, 2004, pp. xii+635. ISBN: 3-540-20488-1 (cit. on p. 71).

[Bis11a] G. Bisson. "Computing endomorphism rings of elliptic curves under the GRH". In: *Journal of Mathematical Cryptology* (2011). arXiv:1101.4323 (cit. on p. 70).

[Bis11b] G. Bisson. “Endomorphism Rings in Cryptography”. PhD thesis. 2011 (cit. on pp. 65, 70, 71).

[BCR10] G. Bisson, R. Cosset, and D. Robert. “AVIsogenies (Abelian Varieties and Isogenies)”. Packet magma dédié au calcul explicite d’isogénies entre variétés abéliennes. 2010. URL: http://avisogenies.gforge.inria.fr. Licence libre (LGPLv2+), enregistré à l’APP (référence IDDN.FR.001.440011.000.R.P.2010.000.10000) (cit. on p. 65).

[BS09] G. Bisson and A. Sutherland. “Computing the endomorphism ring of an ordinary elliptic curve over a finite field”. In: *Journal of Number Theory* (2009) (cit. on p. 70).

[BMS+08] A. Bostan, F. Morain, B. Salvy, and E. Schost. “Fast algorithms for computing isogenies between elliptic curves”. In: *Mathematics of Computation* 77.263 (2008), pp. 1755–1778 (cit. on pp. 34, 70).

[BL09] R. Bröker and K. Lauter. “Modular polynomials for genus 2”. In: *LMS J. Comput. Math.* 12 (2009), pp. 326–339. ISSN: 1461-1570 (cit. on pp. 65, 71).

[BLS09] R. Bröker, K. Lauter, and A. Sutherland. *Modular polynomials via isogeny volcanoes*. 2009. arXiv:1001.0402 (cit. on pp. 14, 70).

[Cer04] J. Cerviño. “On the correspondence between supersingular elliptic curves and maximal quaternionic orders”. In: *Arxiv preprint math/0404538* (2004) (cit. on p. 70).

[CLG09] D. Charles, K. Lauter, and E. Goren. “Cryptographic hash functions from expander graphs”. In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790 (cit. on p. 15).

[CJS10] A. Childs, D. Jao, and V. Soukharev. “Constructing elliptic curve isogenies in quantum subexponential time”. In: *Arxiv preprint arXiv:1012.4019* (2010) (cit. on p. 37).

[CR11] R. Cosset and D. Robert. "An algorithm for computing (ℓ,ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". Mar. 2011. URL: http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991 (cit. on pp. 65, 71).

[Cou94] J. Couveignes. "Quelques calculs en théorie des nombres". PhD thesis. 1994 (cit. on pp. 36, 70).

[Cou96] J. Couveignes. "Computing l-isogenies using the p-torsion". In: *Algorithmic Number Theory* (1996), pp. 59–65 (cit. on pp. 36, 70).

[CDM96] J. Couveignes, L. Dewaghe, and F. Morain. *Isogeny cycles and the Schoof-Elkies-Atkin algorithm*. Tech. rep. Citeseer, 1996 (cit. on p. 70).

[CL08] J. Couveignes and R. Lercier. "Galois invariant smoothness basis". In: *Algebraic geometry and its applications* (2008) (cit. on p. 15).

[CL09] J. Couveignes and R. Lercier. "Elliptic periods for finite fields". In: *Finite fields and their applications* 15.1 (2009), pp. 1–22 (cit. on p. 15).

[CM94] J. Couveignes and F. Morain. "Schoof's algorithm and isogeny cycles". In: *Algorithmic Number Theory* (1994), pp. 43–58 (cit. on p. 70).

[Cox89] D. Cox. *Primes of the form x2+ ny2*. Wiley, 1989 (cit. on p. 70).

[Del69] P. Deligne. "Variétés abéliennes ordinaires sur un corps fini". In: *Inventiones Mathematicae* 8.3 (1969), pp. 238–243 (cit. on p. 71).

[DIK06] C. Doche, T. Icart, and D. Kohel. "Efficient scalar multiplication by isogeny decompositions". In: *Public Key Cryptography-PKC 2006* (2006), pp. 191–206 (cit. on p. 15).

[Dup06] R. Dupont. "Moyenne arithmetico-geometrique, suites de Borchardt et applications". In: *These de doctorat, Ecole polytechnique, Palaiseau* (2006) (cit. on pp. 65, 71).

[EL07] K. Eisentrager and K. Lauter. "A CRT algorithm for constructing genus 2 curves over finite fields". In: *AGCT-11* (2007) (cit. on p. 71).

[Elk92] N. Elkies. "Explicit isogenies". In: *manuscript, Boston MA* (1992) (cit. on p. 70).

[Elk97] N. Elkies. "Elliptic and modular curves over finite fields and related computational issues". In: *Computational perspectives on number theory: proceedings of a conference in honor of AOL Atkin, September 1995, University of Illinois at Chicago*. Vol. 7. Amer Mathematical Society. 1997, p. 21 (cit. on pp. 14, 70).

[Eng09a] A. Enge. "Computing modular polynomials in quasi-linear time". In: *Math. Comp* 78.267 (2009), pp. 1809–1824 (cit. on p. 70).

[Eng09b] A. Enge. "The complexity of class polynomial computation via floating point approximations". In: *Mathematics of Computation* 78.266 (2009), pp. 1089–1107 (cit. on p. 70).

[ES10] A. Enge and A. Sutherland. "Class invariants by the CRT method, ANTS IX: Proceedings of the Algorithmic Number Theory 9th International Symposium". In: *Lecture Notes in Computer Science* 6197 (July 2010), pp. 142–156 (cit. on pp. 14, 70).

[FLR11] J.-C. Faugère, D. Lubicz, and D. Robert. "Computing modular correspondences for abelian varieties". In: *Journal of Algebra* (2011). arXiv:0910.4668. URL: http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf. HAL: hal-00426338. (Cit. on p. 71).

[Feo10a] L. de Feo. "Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic". In: *Journal of Number Theory* (2010) (cit. on pp. 36, 70).

[Feo10b] L. de Feo. "Algorithmes Rapides pour les Tours de Corps Finis et les Isogénies". PhD thesis. Ecole Polytechnique X, Dec. 2010. URL: http://hal.inria.fr/tel-00547034/en (cit. on pp. 37, 70).

[Fou01] M. Fouquet. "http://www.math.jussieu.fr/ fouquet/Manuscrit.ps.gz". PhD thesis. 2001 (cit. on p. 70).

[FM02] M. Fouquet and F. Morain. "Isogeny volcanoes and the SEA algorithm". In: *Algorithmic Number Theory* (2002), pp. 47–62 (cit. on pp. 49, 70).

[FL08] D. Freeman and K. Lauter. "Computing endomorphism rings of Jacobians of genus 2 curves over finite fields". In: *Algebraic Geometry and its Applications, World Scientific* (2008), pp. 29–66 (cit. on p. 71).

[GHS02] S. Galbraith, F. Hess, and N. Smart. "Extending the GHS Weil descent attack". In: *Advances in Cryptology—EUROCRYPT 2002*. Springer. 2002, pp. 29–44 (cit. on p. 13).

[Gau00] P. Gaudry. "Algorithmique des courbes hyperelliptiques et applications à la cryptologie". PhD thesis. École Polytechnique, Dec. 2000 (cit. on pp. 65, 71).

[Gau07] P. Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 15).

[GM07] G. van der Geer and B. Moonen. "Abelian varieties". In: *Book in preparation* (2007) (cit. on p. 71).

[How95] E. Howe. "Principally polarized ordinary abelian varieties over finite fields". In: *American Mathematical Society* 347.7 (1995) (cit. on p. 71).

[IJ10] S. Ionica and A. Joux. "Pairing the volcano". In: *Algorithmic Number Theory* (2010), pp. 201–218 (cit. on p. 71).

[JS10] D. Jao and V. Soukharev. "A subexponential algorithm for evaluating large degree isogenies". In: *Algorithmic Number Theory* (2010), pp. 219–233 (cit. on p. 37).

[JL06] A. Joux and R. Lercier. "Counting points on elliptic curves in medium characteristic". Cryptology ePrint Archive, Report 2006/176. May 2006 (cit. on p. 70).

[Kem89] G. Kempf. "Linear systems on abelian varieties". In: *American Journal of Mathematics* 111.1 (1989), pp. 65–94 (cit. on p. 71).

[KKM09] A. Koblitz, N. Koblitz, and A. Menezes. "Elliptic curve cryptography: The serpentine course of a paradigm shift". In: *Journal of Number Theory* (2009) (cit. on p. 70).

[Koh96] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, 1996 (cit. on p. 70).

[Ler97] R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis. These, LIX–CNRS, juin 1997*. 1997. URL: http://cat.inist.fr/?cpsidt=183634 (cit. on p. 70).

[LS08] R. Lercier and T. Sirvent. "On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field." In: *Journal de théorie des nombres de Bordeaux* 20.3 (2008), pp. 783–797 (cit. on pp. 35, 70).

[LR10] D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". 2010. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf. HAL: hal-00446062 (cit. on pp. 65, 71).

[ML04] K. McMurdy and K. Lauter. "Explicit Generators for Endomorphism Rings of Supersingular Elliptic Curves". In: (2004) (cit. on p. 70).

[Mil85] J. Milne. "Jacobian varieties". In: *Arithmetic geometry (G. Cornell and JH Silverman, eds.)* (1985), pp. 167–212 (cit. on p. 71).

[Mil86] J. Milne. "Abelian varieties". In: *Arithmetic geometry (G. Cornell and JH Silverman, eds.)* (1986), pp. 103–150 (cit. on p. 71).

[Mil91] J. Milne. *Abelian varieties*. 1991. URL: http://www.jmilne.org/math/CourseNotes/av.html (cit. on p. 71).

[MMS+06] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. "An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields". In: *Applied mathematics and computation* 176.2 (2006), pp. 739–750 (cit. on p. 71).

[Mor95] F. Morain. "Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques". In: *J. Théor. Nombres Bordeaux* 7 (1995), pp. 255–282 (cit. on pp. 14, 70).

[Mum66] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on p. 71).

[Mum67a] D. Mumford. "On the equations defining abelian varieties. II". In: *Invent. Math.* 3 (1967), pp. 75–135 (cit. on p. 71).

[Mum67b] D. Mumford. "On the equations defining abelian varieties. III". In: *Invent. Math.* 3 (1967), pp. 215–244 (cit. on p. 71).

[Mum70] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970, pp. viii+242 (cit. on p. 71).

[Mum83] D. Mumford. *Tata lectures on theta I*. Vol. 28. Progress in Mathematics. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Boston, MA: Birkhäuser Boston Inc., 1983, pp. xiii+235. ISBN: 3-7643-3109-7 (cit. on p. 71).

[Mum84] D. Mumford. *Tata lectures on theta II*. Vol. 43. Progress in Mathematics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Boston, MA: Birkhäuser Boston Inc., 1984, pp. xiv+272. ISBN: 0-8176-3110-0 (cit. on p. 71).

[Mum91] D. Mumford. *Tata lectures on theta III*. Vol. 97. Progress in Mathematics. With the collaboration of Madhav Nori and Peter Norman. Boston, MA: Birkhäuser Boston Inc., 1991, pp. viii+202. ISBN: 0-8176-3440-1 (cit. on p. 71).

[Rob10] D. Robert. "Theta functions and applications in cryptography". PhD thesis. Université Henri-Poincarré, Nancy 1, France, July 2010. URL: http://www.normalesup.org/~robert/pro/publications/academic/phd.pdf. Slides http://www.normalesup.org/~robert/pro/publications/slides/2010-07-phd.pdf, TEL: tel-00528942. (Cit. on p. 71).

[RS06] A. Rostovtsev and A. Stolbunov. "Public-key cryptosystem based on isogenies". In: *International Association for Cryptologic Research. Cryptology ePrint Archive* (2006). eprint: http://eprint.iacr.org/2006/145 (cit. on p. 15).

[Sch95] R. Schoof. "Counting points on elliptic curves over finite fields". In: *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254 (cit. on pp. 14, 70).

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate Texts in Mathematics. Corrected reprint of the 1986 original. New York: Springer-Verlag, 1986, pp. xii+400. ISBN: 0-387-96203-4 (cit. on p. 70).

[Sma03] N. Smart. "An analysis of Goubin's refined power analysis attack". In: *Cryptographic Hardware and Embedded Systems-CHES 2003* (2003), pp. 281–290 (cit. on p. 15).

[Smi09] B. Smith. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*. Feb. 2009. arXiv:0806.2995 (cit. on p. 13).

[Sut09] A. Sutherland. "Computing Hilbert class polynomials with the Chinese remainder theorem". In: *Mathematics of Computation* (2009) (cit. on pp. 14, 70).

[Tes06] E. Teske. "An elliptic curve trapdoor system". In: *Journal of cryptology* 19.1 (2006), pp. 115–133 (cit. on p. 15).

[Wag09] M. Wagner. "Über Korrespondenzen zwischen algebraischen Funktionenkörpern". PhD thesis. Technische Universität Berlin, 2009 (cit. on p. 71).

[Wat69] W. Waterhouse. “Abelian varieties over finite fields”. In: *Ann. Sci. Ecole Norm. Sup* 2.4 (1969), pp. 521–560 (cit. on p. 71).

[WM71] W. Waterhouse and J. Milne. “Abelian varieties over finite fields”. In: *Proc. Symp. Pure Math* 20 (1971), pp. 53–64 (cit. on p. 71).