The group structure of rational points of elliptic curves over a finite field

2015/09 — ECC 2015, Bordeaux, France

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest
Institut de Mathématiques de Bordeaux

September 2015

Introduction

- Cryptography!
- We are interested in $E(\mathbb{F}_q)$, were E is an elliptic curve over a finite field $\mathbb{F}_q$;
- References: [Sil86; Len96; Wat69; WM71; Mil06];

Torus

- An elliptic curve $E/\mathbb{C}$ is a torus $E=\mathbb{C}/\Lambda$, where Λ is a lattice $\Lambda=\tau\mathbb{Z}+\mathbb{Z}$, $(\tau\in\mathfrak{H})$.
- 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 (normalised) 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

$$y^2=4x^3-60E_4(\Lambda)-140E_6(\Lambda)=4x^3-g_2(\Lambda)-g_3(\Lambda).$$

- In particular the elliptic functions are rational functions in $\wp,\wp'$: $\mathbb{C}(E)=\mathbb{C}(\wp,\wp')$.
- Two elliptic curves $E=\mathbb{C}/\Lambda$ and $E'=\mathbb{C}/\Lambda'$ are isomorphic if there exists $\alpha\in\mathbb{C}^*$ such that $\Lambda=\alpha\Lambda'$;
- Two elliptic curves are isomorphic if and only if they have the same j-invariant: $j(\Lambda)=j(\Lambda')$.

$$j(\Lambda)=1728\frac{g_2^3}{g_2^3-27g_3^2}.$$

Lattices

- $\wp$ is homogeneous of degree -2 and $\wp'$ of degree -3:

$$\wp(\alpha z, \alpha\Lambda) = \alpha^{-3}\wp(z, \Lambda);$$

- Up to normalisation one has $\Lambda = \tau\mathbb{Z} + \mathbb{Z}$ with $\tau \in \mathfrak{H}_g$ the upper half plane;
- This gives a parametrisation of lattices Λ by $\tau \in \mathfrak{H}_g$;
- If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$ then a new basis of Λ is given by $(a\tau + b, c\tau + d)$;
- We can normalize this basis by multiplying by $(c\tau + d)^{-1}$ to get $\Lambda' = \frac{a\tau+b}{c\tau+d}\mathbb{Z} + \mathbb{Z}$;
- The isomorphism class of elliptic curves is then parametrized by $\mathfrak{H}_g / \mathrm{Sl}_2(\mathbb{Z})$.

Elliptic curves over a field k

Definition

An elliptic curve E/k (k perfect) can be defined as

- A nonsingular projective plane curve E/k of genus 1 together with a rational point $0_E \in E(k)$;
- A nonsingular projective plane curve E/k of degree 3 together with a rational point $0_E \in E(k)$;
- A nonsingular projective plane curve E/k of degree 3 together with a rational point $0_E \in E(k)$ which is a point of inflection;
- A non singular projective curve with equation (the Weierstrass equation)

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

(in this case $0_E = (0:1:0)$);

Choice of the base point

Remark

- If E is a nonsingular projective plan curve of degree 3 and $O \in E(k)$, then if O is an inflection point there is a linear change of variable which puts E into Weierstrass form and $O = (0:1:0)$, but otherwise needs a non linear change of variable to transform O into an inflection point;
- If $\operatorname{char} k > 3$ then a linear change of variable on the Weierstrass equation gives the short Weierstrass equation:

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

Class of isomorphisms of elliptic curves

- The Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

has discriminant $\Delta_E = -b_2b_8 - 8b_3 - 27b_2 + 9b_2b_4b_6$ so it defines an elliptic curve whenever $\Delta_E \neq 0$.
(Here $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$,
$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$).

- The j-invariant of E is

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

- When we have a short Weierstrass equation $y^2 = x^3 + ax + b$, the discriminant is $-16(4a^3 + 27b^2)$ and the j-invariant is

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

Theorem

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

Isomorphisms and Twists

- 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 $s = t = 0$.
- A twist of an elliptic curve E/k is an elliptic curve E'/k isomorphic to E over $\overline{k}$ but not over k.

Example

- Every elliptic curve $E/\mathbb{F}_q : y^2 = x^3 + ax + b$ 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.

The addition law

- Let E be an elliptic curve given by a Weierstrass equation
- Then $(E, 0_E)$ is an abelian variety;
- The addition law is recovered by the chord and tangent law;
- If $k = \mathbb{C}$ this addition law coincides with the one on $\mathbb{C}$ modulo the lattice Λ. (The addition law of an abelian variety is fixed by the base point, and the base point $0 \in \mathbb{C}$ corresponds to the point at infinity of E since $\wp$ and $\wp'$ have a pole at 0).
- For $E : y^2 = x^3 + ax + b$ the addition law is given by

$$P + Q = -R = (x_R, -y_{-R})$$

$$\alpha = \frac{y_Q - y_P}{x_Q - x_P} \quad \text{or } \alpha = \frac{f'(x_P)}{2y_P} \text{ when } P = Q$$

$$x_R = \alpha^2 - x_P - x_Q$$

$$y_{-R} = y_P + \alpha(x_R - x_P)$$

- Indeed write $l_{P,Q} : y = \alpha x + \beta$ the line between P and Q (or the tangent to E at P when $P = Q$). Then $y_{-R} = \alpha x_{-R} + \beta$ and $y_P = \alpha x_P + \beta$ so $y_{-R} = \alpha(x_R - x_P) + y_P$. Furthermore x_R, x_P, x_Q are the three roots of $x^3 + ax + b - (\alpha x + \beta)^2$ so $x_P + x_Q + x_R = \alpha^2$.

Elliptic curves over other fields

- Why look at $\mathbb{C}$? For cryptography we work with elliptic curves over finite fields;
- Everything that is true over $\mathbb{C}$ is true over other fields except when it is not true (non algebraically closed fields, characteristic p...). Example: "there are n^2 points of n-torsion".
- For things that are not true over other fields, change the definition so that it remains true. Examples: "the subscheme $E[n]$ has degree n^2", definition of the Tate module $T_p E$ as a p-divisible group when the characteristic is p...

Elliptic curves over other fields

- Why look at $\mathbb{C}$? For cryptography we work with elliptic curves over finite fields;
- Everything that is true over $\mathbb{C}$ is true over other fields except when it is not true (non algebraically closed fields, characteristic p...). Example: "there are n^2 points of n-torsion".
- For things that are not true over other fields, change the definition so that it remains true. Examples: "the subscheme $E[n]$ has degree n^2", definition of the Tate module $T_p E$ as a p-divisible group when the characteristic is p...

Elliptic curves over other fields

- Why look at $\mathbb{C}$? For cryptography we work with elliptic curves over finite fields;
- Everything that is true over $\mathbb{C}$ is true over other fields except when it is not true (non algebraically closed fields, characteristic p...). Example: "there are n^2 points of n-torsion".
- For things that are not true over other fields, change the definition so that it remains true. Examples: "the subscheme $E[n]$ has degree n^2", definition of the Tate module $T_p E$ as a p-divisible group when the characteristic is p...

Elliptic curves over other fields

- Why look at $\mathbb{C}$? For cryptography we work with elliptic curves over finite fields;
- Everything that is true over $\mathbb{C}$ is true over other fields except when it is not true (non algebraically closed fields, characteristic p...). Example: "there are n^2 points of n-torsion".
- For things that are not true over other fields, change the definition so that it remains true. Examples: "the subscheme $E[n]$ has degree n^2", definition of the Tate module $T_p E$ as a p-divisible group when the characteristic is p...

Transferring results from $\mathbb{C}$ to other fields

- If $\overline{k}$ is an algebraically closed field of characteristic 0 and of cardinality $2^{\aleph}_0$ then $\overline{k}$ is isomorphic to $\mathbb{C}$;
- If $\overline{k}$ is an algebraically closed field of characteristic 0 it is elementary equivalent to $\mathbb{C}$ so the first order statements valid over $\mathbb{C}$ are valid over $\overline{k}$ too;
- If a first order statement is true over $\mathbb{C}$, it is also true for all algebraically closed field of characteristic $p >> 0$ (by compacity arguments);
- If $E/\mathbb{F}_q$ is an elliptic curve over a finite field, it can be lifted to an elliptic curve over $\mathbb{Q}_q$ (and $\mathbb{Q}_q$ is a subfield of $\mathbb{C}_q$ which is isomorphic to $\mathbb{C}$ by the explanation above);
- If $E/\mathbb{F}_q$ is an ordinary elliptic curve, there is a lift to $\mathbb{Q}_q$ which respects $\mathrm{End}(E)$;
- A polynomial in $\mathbb{Z}[X_1, \ldots, X_n]$ which is 0 on a Zariski dense subset of $\mathbb{C}^n$ is identically null.

Example

If $A \in \mathrm{Mat}_n(R)$ is a matrix, then $\mathrm{adj}\ A.A = A.\mathrm{adj}\ A = \det A.\mathrm{Id}$. Indeed this is true for diagonalisable matrices over $\mathbb{C}$ which form a dense Zariski subset (standard linear algebra), so it is true over any ring because the adjoint matrix is given by universal polynomials in the coefficients of A.

Field of definition

- Let E/k be an elliptic curve, and let k_0 be the base field of k;
- There exist an elliptic curve E_0 over $k_0(j(E))$ which is a twist of E;
- E can then be defined over a finite algebraic extension of $k_0(j(E))$;
- $k_0(j(E))$ is either algebraic over k_0 or of transcendance degree 1.

Corollary

Every elliptic curve can be defined over a finite extension of $\mathbb{F}_p(T)$ *or* $\mathbb{Q}(T)$*. If* $\operatorname{char} k = 0$*,* E *can be defined over a subfield of* $\mathbb{C}$*.*

n-torsion over $k = \mathbb{C}$

- $E[n] = \{P \in E(k) \mid n.P = 0_E\}$;
- If $E = \mathbb{C}/\Lambda$, $E[n] = \frac{1}{n}\Lambda/\Lambda$;
- $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$.

n-torsion over $k = \overline{k}$

- Let $\overline{k}$ be an algebraically closed field of characteristic p;
- Let $E : y^2 = x^3 + ax + b$ be an elliptic curve (for simplicity we assume $p = 0$ or $p > 3$);
- Since E has dimension one, $E(\overline{k})$ is infinite (Exercice);
- The subscheme $E[n]$ has dimension 0 and degree n^2;

Proof

- Via division polynomials: there exists a unitary polynomial $\varphi_n(x)$ of degree n^2 such that $[n]P = 0_E$ if and only if $\varphi_n(x_P) = 0$ (Exercice: why does φ_n not depend on y?);
- Via dual isogenies: $[n] : E \to E$ is its own dual isogeny, so $[\deg[n]] = [n] \circ \widehat{[n]} = [n^2]$, and $\deg[n] = n^2$;
- Via divisors: if D is a divisor on E, the theorem of the cube shows that $[n]^*D$ is linearly equivalent to $\frac{n^2+n}{2}D + \frac{n^2-n}{2}[-1]^*D$. But $\deg[n]^*D = \deg[n] \deg D$ so $\deg[n] = \frac{n^2+n+n^2-n}{2} = n^2$.

Group structure of the n-torsion

- $d[n]$ is the multiplication by n map on the tangent space $T_{0_E}E$, so $[n]$ is étale whenever $p \nmid n$;
- In this case $\#E[n](\overline{k}) = n^2$ so $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$ (Exercice);
- Either $\#E[p](\overline{k}) = p$ (in which case E is an ordinary elliptic curve), or $\#E[p](\overline{k}) = 0$ (and E is a supersingular elliptic curve);
- If E is ordinary, $E[p^e] = \mathbb{Z}/p^e\mathbb{Z} \oplus \mu_{p^e}$ where $\mu_p = \operatorname{Spec} \mathbb{Z}[T]/(T^{p^e} - 1)$;
- If E is supersingular, $E[p^e] = \alpha_{p^e}^2$ where $\alpha_{p^e} = \operatorname{Spec} \mathbb{Z}[T]/T^{p^e}$ is connected.

Proof

- Let π be the (small) Frobenius, $\widehat{\pi}$ be the Verschiebung, then π is purely inseparable, and $\pi \circ \widehat{\pi} = [p]$, $\widehat{\pi} \circ \pi = [p]$, $\deg \pi = \deg \widehat{\pi} = p$;
- The Weil pairing e_n shows that $E[n]$ (and in particular $E[p]$) is self-dual;
- If $\widehat{\pi}$ is separable, then $\mathbb{Z}/p\mathbb{Z}$ is a subscheme of $E[p]$ and so is its dual μ_p. Taking degrees yield $E[p] = \mathrm{Ker}\, \widehat{\pi} \oplus \mathrm{Ker}\, \pi = \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$.
- Otherwise $\widehat{\pi}$ is not separable, so $\mathrm{Ker}\, \pi$ cannot be μ_p (because its dual $\mathbb{Z}/p\mathbb{Z}$ would be a subscheme of $E[p]$) which implies that $\mathrm{Ker}\, \pi = \alpha_p$ (α_p is self-dual).

Tate modules

- The ℓ-adic numbers $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$ are a way to handle all the residue rings $\mathbb{Z}/\ell^n\mathbb{Z}$ at once, $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z} = \prod_\ell \mathbb{Z}_\ell$.
- Likewise the Tate modules are a way to encode the (ℓ-primary) torsion subgroup:

$$T_\ell(E) = \varprojlim E[\ell^n](\overline{k})$$
$$T(E) = \varprojlim E[n](\overline{k})$$

- $E[n](\overline{k}) \simeq T(E)/nT(E)$;
- $T_\ell(E) = \mathbb{Z}_\ell^2$ if $p \nmid \ell$;
- If E is ordinary $T_p(E) = \mathbb{Z}_p$, and $T(E) = \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}'$ (where $\widehat{\mathbb{Z}}' = \varprojlim_{p \nmid n} \mathbb{Z}/n\mathbb{Z}$) and $E(\overline{k})_{\mathrm{tors}} = \mathbb{Q}/\mathbb{Z} \oplus \mathbb{Z}_{(p)}/\mathbb{Z}$;
- If E is supersingular $T_p(E) = 0$ and $T(E) = \widehat{\mathbb{Z}}' \times \widehat{\mathbb{Z}}'$ and $E(\overline{k})_{\mathrm{tors}} = \mathbb{Z}_{(p)}/\mathbb{Z} \oplus \mathbb{Z}_{(p)}/\mathbb{Z}$.

The group of rational points over a finite field

- If $k = \mathbb{F}_q$ then $E(k)$ is finite;
- In fact (Exercice):

$$E(k) = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \quad \text{with } n_1 \mid n_2.$$

- We will study how n_1, and n_2 vary under isogenies and fields extensions.

The Weil pairing over $\mathbb{C}$

- $E = \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$;
- The function

$$\begin{array}{rcl} e_n \colon E[n]\times E[n] & \longrightarrow & \mu_n \\ (P,Q) & \longmapsto & e^{2\pi i n\left(x_P y_Q - x_Q y_P\right)} \end{array}$$

  where $P = x_P + \tau y_P$ and $Q = x_Q + \tau y_Q$ is bilinear and non degenerate;
- The value does not depend on the choice of basis for the lattice $\Lambda = \mathbb{Z}+\tau\mathbb{Z}$: let $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, then if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$,

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_P \\ y_P \end{pmatrix}\right)^T J \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_Q \\ y_Q \end{pmatrix}\right) = \begin{pmatrix} x_P \\ y_P \end{pmatrix}^T \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t J \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\begin{pmatrix} x_Q \\ y_Q \end{pmatrix} =$$

$$\begin{pmatrix} x_P \\ y_P \end{pmatrix}^T J \begin{pmatrix} x_Q \\ y_Q \end{pmatrix} = x_P y_Q - x_Q y_P$$

Divisors

- Let C be a projective smooth and geometrically connected curve;
- A divisor D is a formal finite sum of points on C:
  $D = n_1[P_1] + n_2[P_2] + \cdots n_e[P_e]$. The degree $\deg D = \sum n_i$.
- If $f \in k(C)$ is a rational function, then

$$\operatorname{Div} f = \sum_P \operatorname{ord}_P(f)[P]$$

($(O_C)_P$ the stalk of functions defined around P is a discrete valuation ring since C is smooth and $\operatorname{ord}_P(f)$ is the corresponding valuation of f at P).

Example

If $C = \mathbb{P}^1_k$ then $\operatorname{Div} \frac{\prod (X-\alpha_i^{e_i})}{\prod (X-\beta_i^{f_i})} = \sum e_i[\alpha_i] - \sum f_i[\beta_i] + (\sum \beta_i - \sum \alpha_i)\infty$. In particular $\deg \operatorname{Div} f = 0$ and conversely any degree 0 divisor comes from a rational function.

Linear equivalence class of divisors

- For a general curve, if $f \in k(C)$, $\mathrm{Div}(f)$ is of degree 0 but not any degree 0 divisor D comes from a function f;
- A divisor which comes from a rational function is called a principal divisor. Two divisors D_1 and D_2 are said to be linearly equivalent if they differ by a principal divisor: $D_1 = D_2 + \mathrm{Div}(f)$.
- $\mathrm{Pic}\, C = \mathrm{Div}^0\, C / \text{Principal Divisors}$
- A principal divisor D determines f such that $D = \mathrm{Div}\, f$ up to a multiplicative constant (since the only globally regular functions are the constants).

Divisors on elliptic curves

Theorem

Let $D = \sum n_i[P_i]$ be a divisor of degree 0 on an elliptic curve E. Then D is the divisor of a function $f \in \overline{k}(E)$ (ie D is a principal divisor) if and only if $\sum n_i P_i = 0_E \in E(\overline{k})$ (where the last sum is not formal but comes from the addition on the elliptic curve).
In particular $P \in E(\overline{k}) \to [P] - [0_E] \in \mathrm{Jac}(E)$ is a group isomorphism between the points in E and the linear equivalence classes of divisors;

Proof.

- We will give an algorithm (Miller's algorithm) which starts from a divisor $D = \sum n_i[P_i]$ of degree 0 and constructs a rational function f such that D is linearly equivalent to $[\sum n_i P_i] - [0_E]$. If $\sum n_i P_i = 0_E$ then D is principal.
- Conversely we have to show that if $P = \sum n_i P_i \neq 0_E$ then $[P] - [0_E]$ is not principal. But if we had a function f such that $\mathrm{Div}(f) = [P] - [0_E]$, then the morphism $E \to \mathbb{P}^1_{\overline{k}} : x \mapsto (1 : f(x))$ associated to f would be birational. But this is absurd: E is an elliptic curve so it has genus 1, it cannot have genus 0.

$\square$

Rational divisors

- A divisor D over a perfect field is rational if it is stable under the Galois action;
- If $f \in k(E)$ then $\operatorname{Div} f$ is a rational divisor, conversely if $f \in \overline{k}(E)$ and $\operatorname{Div} f$ is rational then there exists $\alpha \in \overline{k}^*$ such that $\alpha f \in k(E)$;
- A linear equivalence class of divisors $[D]$ is rational if it is stable under the Galois action: $\sigma D \sim D \ \forall \sigma \in \operatorname{Gal}(\overline{k}/k)$;
- Over an elliptic curve E, if $D \simeq [P]-[0_E]$ then D is rational if and only if P is rational;
- Over a curve C with $C(k) \neq 0$ then a rational equivalence class of divisors has a representative given by a rational divisor;
- In particular the map $P \mapsto [P]-[0_E]$ is Galois-equivariant.

Miller's functions

- Let $\mu_{P,Q}$ be a function with divisor $[P]+[Q]-[P+Q]-[0_E]$;
- Using the geometric interpretation of the addition law on E one can construct $\mu_{P,Q}$ explicitly:
- if $P=-Q$ then $\mu_{P,Q}=x-x_P$;
- Otherwise let $l_{P,Q}$ be the line going through P and Q (if $P=Q$ then we take $l_{P,Q}$ to be the tangent to the elliptic curve at P). Then $\mathrm{Div}(l_{P,Q})=[P]+[Q]+[-P-Q]-3[0_E]$.
- Let $v_{P,Q}$ be the vertical line going through $P+Q$ and $-P-Q$; $\mathrm{Div}(v_{P,Q})=[P+Q]+[-P-Q]-2[0_E]$;
- $\mu_{P,Q}=\frac{l_{P,Q}}{v_{P,Q}}$;
- Explicitly if $E: y^2=x^3+ax+b$ is given by a short Weierstrass equation,

$$\mu_{P,Q}=\frac{y-\alpha(x-x_P)-y_P}{x+(x_P+x_Q)-\alpha^2} \tag{1}$$

with $\alpha=\frac{y_P-y_Q}{x_P-x_Q}$ when $P\neq Q$ and $\alpha=\frac{f'(x_P)}{2y_P}$ when $P=Q$.

Miller's algorithm: reducing divisors

- Let $D = [P] + [Q] + D_0$ be a divisor of degree 0;
- Using $\mu_{P,Q}$ we get that $D = \mathrm{Div}(\mu_{P,Q}) + [P+Q] + D_0 + [0_E]$;
- We can iterate the reduction until there is only one non zero point in the support: $D = \mathrm{Div}(g) + [R] - [0_E]$;
- D is principal if and only if $R = 0_E$, in which case g is a function (explicitly written in terms of the $\mu_{P,Q}$) with divisor D (and normalised at 0_E).

Miller's algorithm: double and add

- If $D = n[P] - n[0_E]$ one can combine the reduction above with a double and add algorithm;
- let $\lambda \in \mathbb{N}$ and $P \in E(k)$; we define $f_{\lambda,P} \in k(E)$ to be the function normalized at 0_E thus that:

$$\mathrm{Div}(f_{\lambda,P}) = \lambda[P] - [\lambda P] - (\lambda - 1)[0_E].$$

- In particular $D = \mathrm{Div}\, f_{n,P} + [nP] - [0_E]$;
- If $\lambda, \nu \in \mathbb{N}$, we have

$$f_{\lambda+\nu,P} = f_{\lambda,P} f_{\nu,P} \mathbf{f}_{\lambda,\nu,P}$$

  where $\mathbf{f}_{\lambda,\nu,P} := \mu_{\lambda P,\nu P}$ is the function associated to the divisor $[(\lambda+\nu)P] - [(\lambda)P] - [(\nu)P] + [0_E]$ and normalized at 0_E;

Miller's algorithm: example

- Let D be a general divisor of degree 0. How to apply a double and add algorithm to reduce D?
- Write $D = D_1 + 2D_2 + 4D_4 + \dots$.
- Example: $D = 5[P] + 7[Q] - 12[0_E]$;
- Reduce: $[P] + [Q] - 2[0_E] \sim [P+Q] - [0_E]$;
- Double: $2[P+Q] - 2[0_E] \sim [2P+2Q] - [0_E]$;
- Add: $[2P+2Q] + [Q] - 2[0_E] \sim [2P+3Q] - [0_E]$;
- Double: $2[2P+3Q] - 2[0_E] \sim [4P+6Q] - [0_E]$;
- Add: $[4P+6Q] + [P+Q] - 2[0_E] \sim [5P+7Q] - [0_E]$;

Evaluating functions on divisors

- If f is a function with support disjoint from a divisor $D = \sum n_i[P_i]$, then one can define
$$f(D) = \prod f(P_i)^{n_i}$$
- If D is of degree 0, then $f(D)$ depends only on $\operatorname{Div} f$;
- Miller's algorithm allows, given $\operatorname{Div} f$ to compute $f(D)$ efficiently, the data $\operatorname{Div} f$ can then be seen as a compact way to represent the function f.
- Technicality: during the execution of Miller's algorithm we introduce temporary points in the support of the divisors we evaluate, so we may get a zero or a pole during the evaluation even through f has support disjoint to D;
- One way to proceed is to extend the definition of $f(P)$ when $\operatorname{ord}_P(f) = n$ by fixing a uniformiser u_P (a function with simple zero at P), and defining $f(P)$ to be $(f/u_P^{\operatorname{ord}_P(f)})(P)$. Since C is smooth, $\widehat{O_p} = k[[u_P]]$, $f \in k((u_P))$ and $f(P)$ is then the first coefficient in the Laurent expansion of f along u_P.
- For an elliptic curve a standard uniformiser at 0_E is $u = x/y$; a function f is said to be normalised at 0_E if $f(0_E) = 1$. This fixes uniquely f in its equivalence class $\operatorname{Div} f$.

Evaluating functions on divisors: example

Algorithm (Evaluating $f_{r,P}$ on Q)

Input: $r \in \mathbb{N}$, $P = (x_P, y_P) \in E[r](\mathbb{F}_q)$, $Q = (x_Q, y_Q) \in E(\mathbb{F}_{q^d})$.

Output: $f_{r,P}(Q)$ *where* $\mathrm{Div}\, f_{r,P} = r[P] - r[0_E]$.

1. *Compute the binary decomposition:* $r := \sum_{i=0}^{I} b_i 2^i$. *Let* $T = P, f_1 = 1, f_2 = 1$.
2. *For* i *in* $[I..0]$ *compute*
   1. α, *the slope of the tangent of* E *at* T.
   2. $f_1 = f_1^2(y_Q - \alpha(x_Q - x_T) - y_T)$, $f_2 = f_2^2(x_Q + 2x_T - \alpha^2)$.
   3. $T = 2T$.
   4. *If* $b_i = 1$, *then compute*
      1. α, *the slope of the line going through* P *and* T.
      2. $f_1 = f_1^2(y_Q - \alpha(x_Q - x_T) - y_T)$, $f_2 = f_2(x_Q + x_P + x_T - \alpha^2)$.
      3. $T = T + P$.

Return

$$\frac{f_1}{f_2}.$$

The Weil pairing over algebraically closed fields

Theorem

Let E be an elliptic curve, r a number and P and Q two points of r-torsion on E. Let D_P be a divisor linearly equivalent to $[P]-[0_E]$ and D_Q be a divisor linearly equivalent to $[Q]-[0_E]$. Then

$$e_{W,r}(P,Q) = \varepsilon(D_P, D_Q)^r \frac{(rD_P)\cdot(D_Q)}{(rD_Q)\cdot(D_P)} \tag{2}$$

is well defined.
Furthermore the application $E[r]\times E[r] \to \mu_r : (P,Q) \mapsto e_{W,r}(P,Q)$ is a pairing, called the Weil pairing. The pairing $e_{W,r}$ is an alternate pairing, which means that $e_{W,r}(P,Q) = e_{W,r}(Q,P)^{-1}$.

Proof.

An essential ingredient of the proof is Weil's reciprocity theorem: if $f, g \in K(E)$, then

$$f(\mathrm{Div}(g)) = \varepsilon(\mathrm{Div}\, f, \mathrm{Div}\, g) g(\mathrm{Div}(f)).$$

(Note: $\varepsilon(\mathrm{Div}\, f, \mathrm{Div}\, g) = 1$ if the two divisors have disjoint support.) □

Weil's pairing in practice

- Recall that $f_{r,P}$ is the function with divisor $r[P] - r[0_E]$ (and normalised at 0_E) constructed via Miller's algorithm;
- Similarly $f_{r,Q}$ has divisor $r[Q] - r[0_E]$;
- $e_{W,r}(P,Q) = (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)}$;
- If during the execution of Miller's algorithm to evaluate $f_{r,P}(Q)$ we find a pole or a zero, then we know that Q is a multiple of P and that $e_{W,r}(P,Q) = 1$.

Embedding degree

- If $\mathbb{F}_q$ is a finite field, the embedding degree e is the smallest integer such that $\mathbb{F}_{q^e} = \mathbb{F}_q(\mu_r)$;
- Alternatively, if $r = \ell$ is prime, it is the smallest integer such that $r \mid q^e - 1$.
- If $\sigma \in \mathrm{Gal}(\overline{k}/k)$, $e_r(\sigma P, \sigma Q) = \sigma(e(P,Q))$ (by unraveling the definition), so if $P, Q \in k$ then $e(P,Q) \in k$;
- In particular if $E[\ell] \subset E(\mathbb{F}_q)$ and ℓ is prime, then $\ell \mid q - 1$.
- More generally if $E[r] \subset E(\mathbb{F}_q)$ then $\mu_r \subset \mathbb{F}_q$.

Application of the Weil pairing

- Extremely useful for cryptography (MOV attack, pairing-based cryptography);
- For cryptography rather use optimised pairings derived from the Tate pairing;
- Application for the group structure: $P, Q \in E[\ell]$ form a basis of the ℓ-torsion if and only if $e_{W,\ell}(P,Q) \neq 1$ (Exercice: compare the complexity with the naive method);
- More generally: $P, Q \in E[r]$ form a basis of the r-torsion if and only if $e_{W,r}(P,Q)$ is a primitive r-root of unity (Exercice: what is the complexity to check this?);

Remark

If $P, Q \in E[n]$, $e_{W,nm}(P,Q) = e_{W,n}(P,Q)^m$ so the Weil pairings glue together to give a symplectic structure on the Tate module $T(E)$.

The Tate pairing over a finite field

Theorem

Let E be an elliptic curve, r a prime number, $P \in E[r](\mathbb{F}_{q^e})$ a point of r-torsion defined over $\mathbb{F}_{q^e}$ and $Q \in E(\mathbb{F}_{q^e})$ a point of the elliptic curve defined over $\mathbb{F}_{q^e}$. Let D_P be a divisor linearly equivalent of $[P]-[0_E]$ and D_Q be a divisor linearly equivalent of $[Q]-[0_E]$. Then

$$e_{T,r}(P,Q) = \left((r D_P)\cdot(D_Q)\right)^{\frac{q^e-1}{r}} \tag{3}$$

is well defined and does not depend on the choice of D_P and D_Q.
Furthermore the application $E[r](\mathbb{F}_{q^e}) \times E(\mathbb{F}_{q^e})/rE(\mathbb{F}_{q^e}) \to \mu_r : (P,Q) \mapsto e_{T,r}(P,Q)$ is a pairing, called the Tate pairing.

Tate's pairing in practice

- Recall that $f_{r,P}$ is the function with divisor $r[P]-r[0_E]$ (and normalised at 0_E) constructed via Miller's algorithm;
- $e_{T,r}(P,Q)=f_{r,P}(Q)^{\frac{q^e-1}{r}}$;
- If during the execution of Tate's algorithm to evaluate $f_{r,P}(Q)$ we find a pole or a zero, then we use $D_Q=[Q+R]-[R]$ instead (for R a random point in $E(\mathbb{F}_{q^e})$) and evaluate

$$e_{T,r}(P,Q)=\left(\frac{f_{r,P}(Q+R)}{f_{r,P}(R)}\right)^{\frac{q^e-1}{r}};$$

- If $R\in E(\mathbb{F}_q)$ and $e>1$ we have

$$e_{T,r}(P,Q)=f_{r,P}(Q+R)^{\frac{q^e-1}{r}}.$$

Tate pairing and the Frobenius

- The Weil pairing, Tate pairing and the Frobenius are related;
- Let $P \in E[r](\mathbb{F}_{q^e})$ and $Q \in E(\mathbb{F}_{q^e})$. Let $Q_0 \in E[r](\overline{k})$ be any point such that $rQ_0 = Q$;
- $\pi^e Q_0 - Q_0 \in E[r]$ (Exercice)
- $$e_{T,r}(P,Q) = e_{W,r}(P,(\pi^e - 1)Q_0)$$
- If $Q' = Q + rR$ with $R \in E(\mathbb{F}_{q^e})$ then one can choose $Q_0' = Q_0 + R$ so that $(\pi^e - 1)(Q_0) = (\pi^e - 1)(Q_0')$;
- So the value of $e_{T,r}(P,Q)$ depends only on the class of $Q \in E(\mathbb{F}_{q^e})/rE(\mathbb{F}_{q^e})$.

Proof

- The link between the Weil and Tate pairing comes from Weil's reciprocity;
- If $E[r] \subset E(\mathbb{F}_{q^e})$, then $(\pi^e - 1)E[r] = 0$ so $\frac{\pi^e - 1}{r}$ is an endomorphism;
- Since the Weil pairing is non degenerate, to show that the Tate pairing is non degenerate we just need to show that $\frac{\pi^k - 1}{r} : E(\mathbb{F}_{q^e}) \rightarrow E[r]$ is surjective;
- The kernel of $\frac{\pi^k - 1}{r}$ restricted to $E(\mathbb{F}_{q^e})$ is $rE(\mathbb{F}_{q^e})$, so the image is isomorphic to $E(\mathbb{F}_{q^e})/rE(\mathbb{F}_{q^e})$;
- $E(\mathbb{F}_{q^e}) = \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ with $a \mid b$, and since $E(\mathbb{F}_{q^e}) \supset E[r]$, we know that $r \mid a$ and $r \mid b$;
- We deduce that $E(\mathbb{F}_{q^e})/rE(\mathbb{F}_{q^e})$ is isomorphic to $\mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/r\mathbb{Z}$, in particular it has cardinal r^2 so the application is indeed surjective;
- The general case comes from Galois cohomology applied to the exact sequence $0 \rightarrow E[r] \rightarrow E(\overline{k}) \rightarrow E(\overline{k}) -> 0$.

Field of definition of the r-roots of unity

- By the CRT, we may assume that $r = \ell^n$;
- μ_{ℓ^n} lives in $\mathbb{F}_{q^e}$ whenever $v_\ell(q^e - 1) \geqslant n$;
- If $\mu_\ell \notin \mathbb{F}_q$ then $\mathbb{F}_q(\mu_\ell) = \mathbb{F}_{q^e}$ with $e \mid \ell - 1$;
- If $\mu_\ell \in \mathbb{F}_q$, then $v_\ell(q^e - 1) = v_\ell(q-1)$ unless $\ell \mid e$;
- If $\mu_\ell \in \mathbb{F}_q$, $v_\ell(q^\ell - 1) = v_\ell(q-1) + 1$ (except possibly when $\ell = 2$ and $v_\ell(q-1) = 1$ where $v_\ell(q^\ell - 1)$ can increase by more than 1);
- (Hint: write $q^e - 1 = (q-1)(1 + q + q^2 + \cdots + q^{k-1})) = (q-1)(q - 1 + q^2 - 1 + \cdots + q^{e-1} - 1 + e))$.

Endomorphisms and isogenies

- An isogeny is a non constant rational application $\varphi : E_1 \to E_2$ between two elliptic curves E_1 and E_2 that commutes with the addition law;
- A rational application φ is an isogeny if and only if $\varphi(0_{E_1}) = 0_{E_2}$ (and $\varphi \neq 0$);
- An isogeny is surjective on the $\overline{k}$-points and has finite kernel;
- The degree of φ is $[k(E_2) : \varphi^* k(E_1)]$;
- An isogeny $\varphi : E_1 \to E_2$ admits a dual $\widehat{\varphi} : E_2 \to E_1$ such that $\varphi \circ \widehat{\varphi} = [\deg \varphi]$ and $\widehat{\varphi} \circ \varphi = [\deg \varphi]$;
- We write $E_1[\varphi] = \mathrm{Ker}\, \varphi$; $\deg \varphi = \deg E_1[\varphi]$ (as a scheme), $\mathrm{Ker}\, \varphi$ determines φ (up to automorphisms);
- If φ is separable (for instance if $p \nmid \deg \varphi$) then $E_1[\varphi] = \{P \in E_1(\overline{k}) \mid \varphi P = 0_{E_2}\}$ so $\deg \varphi = \# E_1[\varphi](\overline{k})$;
- Conversely a finite subscheme group K determines an isogeny $E \to E/K$ of degree $\deg K$;
- Over an elliptic curve, every isogeny is (up to isomorphisms) the composition of a separable isogeny and a power of the small Frobenius π_p.
- An endomorphism $\varphi \in \mathrm{End}(E)$ is an isogeny from E to E.

Endomorphism and isogenies over $\mathbb{C}$

- Let $E_1 = \mathbb{C}/\Lambda_1$ and $E_2 = \mathbb{C}/\Lambda_2$;
- An isogeny comes from a linear map $z \mapsto \alpha z$ where $\alpha\Lambda_1 \subset \Lambda_2$;
- The kernel is $\alpha^{-1}\Lambda_2/\Lambda_1$;
- If $E = \mathbb{C}/\Lambda$ an endomorphism comes from a linear map $z \mapsto \alpha z$ where $\alpha\Lambda \subset \Lambda$;
- Write $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$, we get that if $\alpha \notin \mathbb{Z}$ then τ satisfy a quadratic equation and $\alpha \in \mathbb{Z}[\tau]$;
- $\mathbb{Q}(\tau)$ is then a quadratic imaginary field and $\mathrm{End}(E)$ an order (because it stabilizes a lattice).

Field of definition of endomorphisms

- Let E/k be an elliptic curve (k perfect);
- It may happen that endomorphisms of E are defined over a larger field than k (Exercice: but there are always defined over a finite extension of k);
- We let $\mathrm{End}(E) = \mathrm{End}_{\overline{k}}(E)$ and $\mathrm{End}_k(E)$ the subring of rational endomorphisms;
- $\varphi \in \mathrm{End}(E)$ is defined over k if and only if it is stable under $\mathrm{Gal}(\overline{k}/k)$;
- In particular if $k = \mathbb{F}_q$ and π is the Frobenius, then $\mathrm{End}_k(E)$ is the commutant of π in $\mathrm{End}(E)$.
- If l/k is an extension of field, then $\mathrm{End}_l(E)/\mathrm{End}_k(E)$ is torsion free (Exercice: if $m\varphi$ is rational, then so is φ).

Remark

If k is not perfect and l/k is a purely inseparable extension of k then $\mathrm{End}_l(E) = \mathrm{End}_k(E)$.

Characteristic polynomial

Let $\varphi \in \mathrm{End}_k(E)$, the characteristic polynomial $\chi_\varphi \in \mathbb{Z}[X]$ is defined as

- The characteristic polynomial of φ on $T_\ell(E)$ ($\ell \neq p$);
- The only polynomial such that $\deg(\varphi - n\,\mathrm{Id}) = \chi_\varphi(n) \quad \forall n \in \mathbb{Z}$;
- If $\mathrm{End}_k(E)$ is quadratic, as the characteristic polynomial of φ in $\mathrm{End}(E)$;
- If $\varphi \notin \mathbb{Z}$, as the characteristic polynomial of φ in $\mathbb{Q}(\varphi)$;
- If $\varphi \in \mathbb{Z}$, as $X^2 - 2\varphi X + \varphi^2$;
- Let $\mathrm{Tr}(\varphi) = \varphi + \hat{\varphi} \in \mathbb{Z}$ and $N(\varphi) = \varphi\hat{\varphi} = \deg\varphi \in \mathbb{Z}$;

$$\chi_\varphi = X^2 - \mathrm{Tr}(\varphi)X + N(\varphi);$$

Corollary

If $p \nmid n$, the characteristic polynomial of φ acting on $E[n]$ is $\chi_\varphi \mod n$.

Remark

If $\varphi \in \mathrm{End}_k(E)$, $\widehat{\varphi} = \overline{\varphi}$.

Characteristic polynomial of the Frobenius ($k = \mathbb{F}_q$)

- $\chi_\pi = X^2 - tX + q$;
- The roots of χ_π in $\mathbb{C}$ have absolute value $|\sqrt{q}|$ so $|t| \leqslant 2\sqrt{q}$ (Hasse);
- $\#E(\mathbb{F}_q) = \deg(\pi - 1) = \chi_\pi(1)$;
- $$\zeta_E = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right) = \frac{1 - tT + qT^2}{(1-qT)(1-T)};$$
- $\chi_{\pi^n} = \mathrm{Res}_X(\chi_\pi(Y), Y^n - X)$;

Theorem (Tate)

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

Action of the Frobenius on $E[\ell]$

- Let $\Delta_\pi = t^2 - 4q$;
- If $\Delta_\pi = 0 \mod \ell$ then either $\pi = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ on $E[\ell]$ (and all ℓ-isogenies are rational) or $\pi = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ (and there is one rational ℓ-isogeny);
- If $\left(\frac{\Delta_\pi}{\ell}\right) = 1$ then $\pi = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ on $E[\ell]$ with $\lambda \neq \nu \in \mathbb{F}_\ell$, $\lambda\mu = q$ (and there are two rational ℓ-isogenies);
- If $\left(\frac{\Delta_\pi}{\ell}\right) = -1$ then $\pi = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ on $E[\ell]$ with $\lambda \neq \nu \in \mathbb{F}_{\ell^2}$, $\lambda\mu = q$ (and there are no rational ℓ-isogenies).

Corollary

If $\ell \,||\, \#E(\mathbb{F}_q)$ then

- *If the embedding degree $e > 1$ then $\pi = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$ and $E[\ell] \subset E(\mathbb{F}_{q^e})$;*
- *Otherwise $\pi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $E[\ell] \subset E(\mathbb{F}_{q^\ell})$.*

Isogenies and Tate modules

- Let $\ell \neq p$ then $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell E_1, T_\ell E_2)$ is injective [Sil86][Theorem III.7.4] (Exercice: show that $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell E_1, T_\ell E_2)$ is injective);
- In particular $\mathrm{End}(E)$ has rank at most 4;

Theorem (Tate,Faltings)

If k is a finite field or a number field, then

$$\mathrm{Hom}_k(E_1, E_2) \otimes \mathbb{Z}_\ell \simeq \mathrm{Hom}_{\mathbb{Z}_\ell(\mathrm{Gal}(\overline{k}/k))}(T_\ell E_1, T_\ell E_2)$$

Remark

Tate's theorem remain valid for $\ell = p$ when considering the Tate module coming from the duality of p-divisible group schemes.

Endomorphism rings and endomorphism fields

$\mathrm{End}_k(E)$ is either

- $\mathbb{Z}$;
- An order in a quadratic imaginary field;
- A maximal order in the definite quaternion algebra ramified at p and ∞.

Remark

If E is an elliptic curve over a finite field $\mathbb{F}_q$, then

- If E is ordinary then $\mathrm{End}(E)$ is an order in a quadratic imaginary field;
- If E is supersingular then $\mathrm{End}(E)$ is a maximal order in the definite quaternion algebra ramified at p and ∞.

Exercice

- In characteristic 0, $\mathrm{End}_k(E)$ is commutative;
- In characteristic p, $\mathrm{End}_k(E) = \mathbb{Z}$ if and only if $j(E)$ is transcendental.

$\mathrm{End}_k^0(E)$

We follow https://rigtriv.wordpress.com/2009/05/14/endomorphisms-of-elliptic-curves-and-the-tate-module/

Lemma

$\mathrm{Hom}(E_1, E_2)$ is torsion free.

Proof.

The degree is multiplicative, so if $[m] \circ f = 0$ then $m = 0$ or $f = 0$. □

Lemma

$\mathrm{End}_k(E)$ has no zero divisors, so $\mathrm{End}_k^0(E) = \mathrm{End}_k(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra

Proof

(We assume here that $p>2$)

- If $\mathrm{End}_k(E)$ has rank 1 then it is $\mathbb{Z}$ (the maximal order of $\mathbb{Q}$);
- Let $\varphi \in \mathrm{End}_k(E) \setminus \mathbb{Z}$, by translating by an integer we can assume that $\mathrm{Tr}\,\varphi = 0$, and since $N(\varphi) = \deg \varphi > 0$ we get that $\mathbb{Z}+\mathbb{Z}\varphi$ is an order in a quadratic imaginary field. If the rank of $\mathrm{End}_k(E) = 2$ then $\mathrm{End}_k(E)$ is an order containing $\mathbb{Z}+\mathbb{Z}\varphi$.
- Otherwise $\psi \mapsto \varphi\psi\varphi^{-1}$ is a linear map of order 2. If ψ is in the -1-eigenspace (Exercice: why does such a ψ exists?) then $(1,\varphi,\psi,\varphi\psi)$ forms a basis of $\mathrm{End}_k(E)$. Thus $\mathrm{End}_k^0(E)$ is a quaternion algebra and $\mathrm{End}_k(E)$ an order in the quaternion algebra.
- Over $\ell \neq p$ we get that $\mathrm{End}_k E \otimes \mathbb{Z}_\ell \subset \mathrm{End}(T_\ell E) = M_2(\mathbb{Z}_\ell)$ so $\mathrm{End}_k^0 E$ is split at ℓ;
- So either $\mathrm{End}_k^0 E = M_2(\mathbb{Q})$ or the definite quaternion algebra ramified at p and ∞. But $M_2(\mathbb{Q})$ has zero divisors so it cannot be $\mathrm{End}_k(E)$.

Endomorphism rings over $\mathbb{F}_q$

- Let $E/\mathbb{F}_q$ be an elliptic curve, π the Frobenius and $\chi_\pi = X^2 - tX + q$;
- E is supersingular if and only if t is not prime to p, if and only if a power of π is an integer, if and only if $\mathrm{End}^0(E)$ is a quaternion algebra if and only if the isogeny class (up to isomorphism) over $\overline{k}$ is finite.
- Either χ_π is irreducible or $\chi_\pi = X^2 - 2 \pm \sqrt{q}X + q = (X \mp \sqrt{q})^2$ and $\pi = \pm\sqrt{q} \in \mathbb{Z}$. If χ_π is irreducible then $\mathrm{End}_k^0 = \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{t^2 - 4q})$ is quadratic imaginary, otherwise End_k^0 is the definite quaternion algebra ramified at p and ∞;
- If E is ordinary over $\mathbb{F}_q$, then $\mathrm{End}_k(E) = \mathrm{End}(E)$ is an order in $\mathbb{Q}(\pi)$ containing $\mathbb{Z}[\pi]$, $\mathbb{Z}[\pi]$ is maximal at p and p splits.
- If E is supersingular, then $\mathrm{End}_k^0(E)$ is a quaternion algebra if and only if $\pi \in \mathbb{Z}$, and $\mathrm{End}_k(E) = \mathrm{End}(E)$ is then a maximal order. Otherwise $\mathrm{End}_k(E)$ is a quadratic order in $\mathbb{Q}(\pi)$ and is maximal at p (even though $\mathbb{Z}[\pi]$ may not be maximal at p).

Proof (partial)

- If E is supersingular then $\pi_p^2 E \simeq E$. In particular $j_E \in \mathbb{F}_{p^2}$ and $\pi_p^2 = [p] \circ \zeta$ where ζ is an automorphism. ζ is then a root of unity in $\mathrm{End}(E)$ so a power of π is an integer. Reciprocally if $\pi^n \in \mathbb{Z}$ then $p \mid \pi^n$ is inseparable so E is supersingular.
- t is not prime to $p \iff$ a power of π is an integer (Not trivial exercice, see [Wat69][Chapter 4]);
- $\pi^n \in \mathbb{Z} \iff \mathrm{End}^0_{\mathbb{F}_{q^n}}(E)$ is a quaternion algebra (by Tate's theorem);
- If $\mathrm{End}^0(E) = \mathbb{Q}(\pi)$ is a quadratic field, then the isogeny class is infinite (Exercice: look at isogenies $E \to E_i$ of degree a prime ℓ_i inert in O_K and prove that the E_i are non isomorphic). Conversely all supersingular elliptic curves are defined over $\mathbb{F}_{p^2}$ so the isogeny class is finite.

Reduction and lifting

- Let O be an order in a imaginary quadratic field K. Then there 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 $\mathrm{End}(E') = O$.*

Automorphisms and twist

- The automorphisms of E are the inversible elements in $O = \mathrm{End}_k E$.
- 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.

Remark

If E_1 is isogeneous to E_2 over k and $k \subset l$, $\mathrm{Hom}_k(E_1, E_2) = \mathrm{Hom}_l(E_1, E_2)$ when $\mathrm{End}_k(E_1) = \mathrm{End}_l(E_2)$. In particular a twist to E is never isogenous to E over k if E is ordinary.

Isogeny class of elliptic curves over $\mathbb{F}_q$

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:

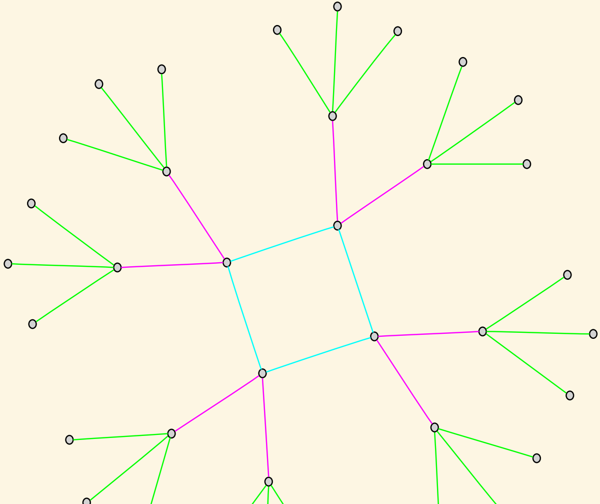
- t prime to p, in this case the isogeny class is ordinary.
- The other cases give supersingular elliptic curves. The endomorphism fraction ring $\mathrm{End}_k^0(\mathscr{E})$ of the isogeny class is either a quaternion algebra of rank 4, or an imaginary quadratic field. In the latter case, it will 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 $\mathrm{End}_k^0(\mathscr{E})$ 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 $d = 6$.

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.

Isogeny graph and endomorphisms of ordinary elliptic curves

The ℓ-isogeny graph looks like a volcano [Koh96; FM02]:
Let f_E be the conductor of $\mathrm{End}(E) \subset O_K$. At each level $v_\ell(f_E)$ increase by one.
At the crater $v_\ell(f_E) = 0$ and at the bottom $v_\ell(f_E) = v_\ell(f) = v_\pi$ where f is the conductor of $\mathbb{Z}[\pi] \subset O_K$.



The α-torsion as an $\mathrm{End}_k(E)$ module

Theorem ([Len96])

- *If* $\mathrm{End}_k(E)$ *is commutative, let* $\alpha \in \mathrm{End}_k(E)$ *be a separable endomorphism. We have an isomorphisme of* $\mathrm{End}_k(E)$*-modules:*

$$E[\alpha] \simeq \mathrm{End}_k(E)/\alpha\,\mathrm{End}_k(E).$$

- *If* $\mathrm{End}_k(E)$ *is non commutative (ie* $\pi \in \mathbb{Z}$*), let* $n \in \mathbb{Z}$*. We have an isomorphism of* $\mathrm{End}_k(E)$*-modules:*

$$E[n] \oplus E[n] \simeq \mathrm{End}_k(E)/n\,\mathrm{End}_k(E).$$

Outline of the proof in the commutative case.

$\mathrm{End}_k(E)$ is a quadratic order so it is a Gorenstein ring. $E[\alpha]$ is faithful over $\mathrm{End}_k(E)/\alpha\,\mathrm{End}_k(E)$, which is a finite Gorenstein ring. So $E[\alpha]$ contains a free $\mathrm{End}_k(E)/\alpha\,\mathrm{End}_k(E)$ module of rank 1, but $\#E[\alpha] = \#\mathrm{End}_k(E)/\alpha\,\mathrm{End}_k(E) = \deg\alpha$ so $E[\alpha]$ is free of rank 1 over $\mathrm{End}_k(E)/\alpha\,\mathrm{End}_k(E)$. □

The structure of the rational points

Theorem (Lenstra)

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve (or suppose that $\pi \notin \mathbb{Z}$). We have as $\mathrm{End}_{\mathbb{F}_q}(E)$-modules:

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

- Let $\Delta_\pi = t^2 - 4q$ and Δ the discriminant of $\mathbb{Q}(\sqrt{\Delta_\pi})$. We have $\Delta_\pi = \Delta f^2$ where f is the conductor of $\mathbb{Z}[\pi] \subset O_K$.
- In practice if $\Delta_\pi = d f_0^2$, then $\Delta = d, f = f_0$ if $d \equiv 1 \mod 4$ or $\Delta = 4d, f = f_0/2$ otherwise;
- Let $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \mod 4$ and $\omega = \sqrt{d}$ otherwise.
- $O_K = \mathbb{Z} \oplus \mathbb{Z}\omega = \mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$;
- $\pi = a + f\omega$ with $a = \frac{t-f}{2}$ if $d \equiv 1 \mod 4$ and $a = \frac{t}{2}$ otherwise;
- Let f_E be the conductor of $\mathrm{End}(E) \subset O_K$, $f_E \mid f$ since $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$, $f = f_E\gamma$ where $\gamma_E = [\mathrm{End}(E) : \mathbb{Z}[\pi]]$;
- $E(\mathbb{F}_q) = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$ where $n_1 \mid n_2$, $n_1 = \gcd(a-1, \gamma_E)$ and $N = n_1 n_2 = \#E(\mathbb{F}_q)$.

Torsion and conductor of the order

Lemma ([MMS+06])

Let $N = n_1 n_2 = \#E(\mathbb{F}_q)$, $\pi = a + f\omega$, $n_1 = \gcd(a-1, \gamma_E)$.

$$v_\ell(a-1) \geqslant \min(v_\ell(f), v_\ell(N)/2).$$

Proof.

$N = \chi_\pi(1) = (1-\pi)(1-\widehat{\pi})$.
If $d \not\equiv 1 \mod 4$, from $\pi = a + f\omega$ we get

$$N = (a-1)^2 - d f^2$$

so $2v_\ell(a-1) \geq \min(2v_\ell(f), v_\ell(N))$.
If $d \equiv 1 \mod 4$, then $(t-2)^2 = f^2 + 4N$ so $4(a-1)^2 = 4N + f^2(d-1) - 4f(a-1)$, and taking valuations yield the Lemma too. $\square$

Corollary

- *If* $v_\ell(n_1) < v_\ell(N)/2$ *then* $v_\ell(\gamma_E) = v_\ell(n_1)$;
- *If* $v_\ell(n_1) = v_\ell(N)/2$ *then* $v_\ell(\gamma_E) \geqslant v_\ell(N)/2$.

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

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

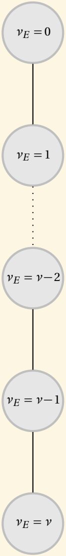
Corollary

When $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^\alpha \oplus \mathbb{Z}/\ell^{m-\alpha}$ with $\alpha \neq m/2$ we can read the ℓ-valuation of the conductor of $\mathrm{End}_k(E)$ directly from the rational points!

Example

If $\ell \,||\, \#E(\mathbb{F}_q)$ then $\mathrm{End}_k(E)$ is maximal at ℓ and the volcano has height 1.

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



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

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

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

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

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

Torsion and extensions

- $v_\ell(f_{\pi^e}) = v_\ell(f_\pi)$ when $\ell \nmid e$;
- $v_\ell(f_{\pi^\ell}) = v_\ell(f_\pi) + 1$, except when $\ell = 2$ and $v_\ell(f_{\pi)} = 1$ when the height can increase by more than one [Fou01];
- If $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{n_1} \oplus \mathbb{Z}/\ell^{n_2}$ $(n_1 \leqslant n_2)$ with $n_1 > 0$ and $n_2 > 0$ then $E[\ell^\infty](\mathbb{F}_{q^e}) = E[\ell^\infty](\mathbb{F}_q)$ when $\ell \nmid e$;
- With the hypothesis above, if $\ell > 2$, $E[\ell^\infty](\mathbb{F}_q^\ell) = \mathbb{Z}/\ell^{n_1+1} \oplus \mathbb{Z}/\ell^{n_2+1}$;
- If $\ell = 2$, n_1 and n_2 can increase by more than one (but when $v_\ell(f_\pi) > 1$ then n_1 only increase by 1) [IJ13].

Number fields

- If K is a number field, $E(K)$ is finitely generated (Mordell);
- $E(\mathbb{Q})_{\text{tors}} \in \{\mathbb{Z}/n\mathbb{Z} \quad 1 \leqslant n \leqslant 10 \text{ or } n = 12\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}\}$ (Mazur).

$E(\overline{k})$ [Len96]

- $E(\overline{k}) = E(\overline{k})_{\mathrm{tors}} \oplus E(\overline{k})/E(\overline{k})_{\mathrm{tors}}$;
- $E(\overline{k})/E(\overline{k})_{\mathrm{tors}}$ is equal to 0 if $\overline{k}$ is the algebraic closure of a finite field, otherwise it is isomorphic as en $\mathrm{End}(E)$ module to $\mathrm{End}^0(E)^{\# k}$;
- Let $\mathfrak{p}$ denotes the endomorphisms acting trivially on the tangeant space $T_0(E)$;
- If E is ordinary ($\operatorname{rank}\mathrm{End}(E) = 2$), $E(\overline{k})_{\mathrm{tors}} = \mathrm{End}(E)_{\mathfrak{p}}/\mathrm{End}(E)$;
- Otherwise ($\operatorname{rank}\mathrm{End}(E) = 4$) $E(\overline{k})_{\mathrm{tors}} \oplus E(\overline{k})_{\mathrm{tors}} = \mathrm{End}(E)_{\mathfrak{p}}/\mathrm{End}(E)$.

Corollary

$E(\overline{k}) = E(\overline{k})_{\mathrm{tors}}$ *if and only if* $\overline{k}$ *is algebraic over a finite field.*

Proof.

If $\overline{k}$ is algebraic over a finite field and $P \in E(\overline{k})$, the coordinates of P are defined over a finite field, so P is of torsion.
Conversely we may assume that $\overline{k}$ is algebraic over $\mathbb{F}_p(T)$ or $\mathbb{Q}$ or $\mathbb{Q}(T)$. If $E(\overline{k}) = E(\overline{k})_{\mathrm{tors}}$ the Jordan-Hölder factors of the absolute Galois group would be of the form $\mathrm{PSL}_2(\mathbb{F}_q)$ (up to a finite number of exceptions). But $\mathbb{F}_p(T)$, $\mathbb{Q}$ and $\mathbb{Q}(T)$ all have Galois extension with the symmetric groups S_n for all n. $\square$

Bibliography

M. Fouquet and F. Morain. "Isogeny volcanoes and the SEA algorithm". In: *Algorithmic Number Theory* (2002), pp. 47–62 (cit. on p. 58).

M. Fouquet. "Anneau d'endomorphismes et cardinalité des couples elliptiques: aspects algorithmiques". PhD thesis. Palaiseau, Ecole Polytechnique, 2001 (cit. on p. 64).

S. Ionica and A. Joux. "Pairing the volcano". In: *Mathematics of Computation* 82.281 (2013), pp. 581–603 (cit. on p. 64).

D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, 1996 (cit. on p. 58).

H. Lenstra Jr. "Complex multiplication structure of elliptic curves". In: *journal of number theory* 56.2 (1996), pp. 227–241 (cit. on pp. 2, 59, 66).

J. Milne. "Elleptic Curves". In: (2006) (cit. on p. 2).

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. 61).

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 pp. 2, 49).

W. Waterhouse. "Abelian varieties over finite fields". In: *Ann. Sci. Ecole Norm. Sup* 2.4 (1969), pp. 521–560 (cit. on pp. 2, 54).

W. Waterhouse and J. Milne. "Abelian varieties over finite fields". In: *Proc. Symp. Pure Math* 20 (1971), pp. 53–64 (cit. on p. 2).