Elliptic Curves 5

Damien Robert[1,2]

[1]Inria Bordeaux Sud Ouest [2]Univesité de Bordeaux

06 November 2020

The Weil pairing

- The Weil pairing is a non degenerated bilinear pairing $e_{W,\ell} : E[\ell] \times E[\ell] \to \mu_\ell$
- $e_{W,\ell}(P,Q) = (-1)^\ell \frac{f_{\ell,P}((Q)-(0_E))}{f_{\ell,Q}((P)-(0_E))}$ where $div f_{\ell,P} = \ell(P) - \ell(0_E)$.
- $e_{W,\ell}(P,Q) = \frac{f_{\ell,P}(Q)}{f_{\ell,Q}(P)}$ if the functions $f_{\ell,P}$ and $f_{\ell,Q}$ are normalised at 0_E.

Uniformisers and valuations

- If $P = (x_P, y_P)$, $y_P \neq 0$, a uniformiser is $\pi_P = x - x_P$.
- If $g(x,y) = g_1(x) + y g_2(x)$, $g(x) = (x - x_P)^n g_1'(x) + y g_2'(x)$, then $v_P(g) = n + v_{x_P} N(g')$.
- If $P = (x_P, 0)$ a Weierstrass point, a uniformiser is $\pi_P = y$.
- If $g(x,y) = g_1(x) + y g_2(x)$, $v_P(g) = \min(2v_{x_P}(g_1), 1 + 2v_{x_P}(g_2))$. Ex: $v_P(x - x_P) = 2$.
- If $P = 0_E$, a uniformiser is $\pi_P = x/y$.
- $v_P(g) = -\deg(g)$ with $\deg(x) = 2$ and $\deg(y) = 3$.

Divisors

Definition

- Let C/k be a smooth curve. A divisor D is a (finite) formal sum of points in $C(\bar{k})$:
$$D = n_1(P_1) + \cdots + n_k(P_k).$$
- The degree of D is $\deg D = \sum n_i$.
- There is an obvious group law on divisors: if $D_1 = \sum n_i(P_i)$, $D_2 = \sum m_i(P_i)$, $D_1 + D_2 = \sum (n_i + m_i)(P_i)$. The zero divisor is $D = 0$.
- The support of D is $\{P_1, \ldots, P_k\}$ where $n_i \neq 0$.

Example

- If $C = \mathbb{P}^1$, $D = (0) + 2(1) - 3(\infty)$ if of degree 0.
- $D = 3(0) + 2(1)$ is of degree 5.

Principal divisors

Definition

If $f \in k(C)$, its associated divisor is

$$div(f) = \sum_{P \in C(\bar{k})} v_P(f)(P).$$

Example

- If $C = \mathbb{P}^1, f = x(x-1)^2, div(f) = (0) + 2(1) - 3(\infty)$.
- If $C = \mathbb{P}^1, f = x^3/(x-2)^4, div(f) = 3(0) - 4(2) + 1(\infty)$.
- If $C = \mathbb{P}^1$, $D = 3(0) + 2(1)$ does not come from a f.
- If $E : y^2 = h(x)$ is an elliptic curve, $f = y$, $div f = (P_1) + (P_2) + (P_3) - 3(\infty)$, where P_1, P_2, P_3 are the three Weierstrass points.
- If $f = x, div(f) = (\sqrt{(}h(0))) + (-\sqrt{(}h(0))) - 2(\infty)$.
- $div(\bar{f}) = \overline{div(f)}$.

Principal divisors

Theorem

If $D = div(f)$, $\deg(D) = 0$.

Proof.

If $C = \mathbb{P}^1, f = \prod(x - a_i)^{n_i}, div(f) = \sum n_i(a_i) - (\sum a_i)(\infty)$,
$\deg div f = \sum n_i - \sum n_i = 0$.
If $C = E$, and P is not a Weierstrass point,
$v_P(f) + v_{-P}(f) = v_P(f) + v_P(\bar{f}) = v_P(Nf) = v_{x_P}(Nf)$. If P is a Weierstrass point, $v_P(f) = v_P(\bar{f})$, so $v_P(Nf) = 2v_P(f)$, but $v_P(Nf) = 2v_{x_P}(Nf)$ since $v_P(x - x_P) = 2$, so $v_P(f) = v_{x_P}(Nf)$. We get that $\deg div_E f = \sum v_P(f) = \sum v_{x_P}(Nf) = \deg div_{\mathbb{P}^1} N(f) = 0$. □

Principal divisors

Proposition

If $div f_1 = div f_2$*, then* $f_1 = \lambda f_2, \lambda \in k^*$.

Proof.

$div f_1 - div f_2 = div(f_1/f_2) = 0$. So $g = f_1/f_2$ has no zeroes nor poles. If $C = \mathbb{P}^1$, then it is easy to check that g is constant. If $C = E$, then Ng has no zeroes nor poles on $\mathbb{P}^1$, so is constant, so g is constant. □

In other word: a function f is completely determined, up to a constant, by its divisor $D = div f$.

Principal divisors

- D is principal if $D = div f$;
- D_1 is linearly equivalent to D_2 if $D_1 - D_2$ is principal: $D_1 = D_2 + div f$. Notation: $D_1 \simeq D_2$.
- D is principal $\leftrightarrow$ D is linearly equivalent to 0. Notation: $D \simeq 0$.

Principal divisors on $\mathbb{P}^1$

Proposition

If $C = \mathbb{P}^1$, D *is principal iff* $\deg D = 0$.

Proof.

D principal $\Rightarrow \deg D = 0$ is true for all curves. Conversely, if $D = \sum n_i(a_i) + m(\infty)$, then $m = -\sum n_i$ since $\deg D = 0$, so we take $f = \prod (x - a_i)^{n_i}$. □

Remark

A (proper smooth) curve C *is isomorphic to* $\mathbb{P}^1$ *iff there is a rational function such that* $div f = (P) - (Q)$, $P \neq Q$. *Indeed* $f : C \to \mathbb{P}^1$ *is an isomorphism which sends* P *to* 0 *and* Q *to* ∞.

Principal divisors on elliptic curves

Definition

Let $D = \sum n_i (P_i)$ be a divisor of degree 0 on an elliptic curve E. We define $[D] = \sum n_i P_i \in E$, the realisation of D in E.

Theorem

A divisor D on E is principal if and only if $\deg D = 0$ and $[D] = 0_E$.

Corollary

If $\deg D = 0$, $D \simeq ([D]) - (0_E)$.

Proof.

Miller's algorithm gives an explicit function f_D whose divisor is $D - ([D]) + (0_E)$. It remains to show that $D = (P) - (0_E)$ cannot be principal if $P \neq 0_E$. But if it was, then E would be isomorphic to $\mathbb{P}^1$. $\square$

Principal divisors on elliptic curves

- If $D = \sum n_i (P_i)$ with $\deg D = \sum n_i = 0$ and $[D] = \sum n_i P_i = 0_E$, then D is principal, so we define f_D a function such that $D = div\, f_D$;
- f_D is determined up to a constant. We can completely normalise f_D by asking that $f_D(0_E) = 1$. This is valid iff 0_E is not a pole or a zero of D.
- More generally, if $m = v_{0_E}(D)$, we can ask that $\left(f_D / \pi_{0_E}^m \right)(0_E) = 1$.
- If $D = \sum n_i (P_i)$ is any divisor, then $D' = D - ([D]) - (\deg D - 1)(0_E)$ is principal. We define $f_D = f_{D'}$.
- If $D = (P) + (-P) - 2(0_E)$, $f_D = x - x_P$.
- If P is a point of ℓ-torsion, $\ell(P) - \ell(0_E)$ is principal, and we define $f_{\ell,P}$ be its normalised function.
- More generally, we let $f_{\ell,P}$ be normalised such that $div\, f_{\ell,P} = \ell(P) - (\ell P) - (\ell - 1)(0_E)$.

Miller's algorithm

- We let $\mu_{P,Q}$ the normalised function such that

$$div\, \mu_{P,Q} = (P) + (Q) - (P+Q) - (0_E).$$

- If $D = (P) + (Q) + D_1$, then $D \simeq (P+Q) - (0_E) + D_1$ via $D = div(\mu_{P,Q}) + (P+Q) - (0_E) + D_1$.
- If $D_1 = R + D_2$, $D = div(\mu_{P,Q}) + div(\mu_{P+Q,R})(P+Q+R) - (0_E) + D_2 = div(\mu_{P,Q}\mu_{P+Q,R}) + (P+Q+R) - (0_E) + D_2$.
- We reduce D until D is of the form $(P) - (0_E)$. D is principal iff $P = 0_E$, in which case the algorithm gives us f_D.

$\mu_{P,Q}$ on $E : y^2 = x^3 + ax + b$

- If $P = -Q$, $\mu_{P,Q} = (x - x_P)$.
- Otherwise, $\mu_{P,Q} = \frac{l_{P,Q}}{v_{P+Q}}$ where $l_{P,Q}$ is the line going through P and Q (or the tangent line at P if $P = Q$), and v_{P+Q} is the vertical line going through $P + Q$.
- Let $R = -P - Q$ be the third point of intersection of $l_{P,Q}$.
- $l_{P,Q} = y - y_P - \alpha(x - x_P)$, $\alpha = \frac{y_Q - y_P}{x_Q - x_P}$ or $\frac{3x_P^2 + a}{2y_P}$;
- $div\, l_{P,Q} = (P) + (Q) + (R) - 3(0_E)$.
- $v_{P+Q} = x - x_{P+Q}$
- $div\, v_{P+Q} = (R) + (-R) - 2(0_E) = (-P - Q) + (P + Q) - 2(0_E)$.
- $\mu_{P,Q} = \frac{y - y_P - \alpha(x - x_P)}{x - x_{P+Q}} = \frac{y - y_P - \alpha(x - x_P)}{x + x_P + x_Q - \alpha^2}$;
- $div\, \mu_{P,Q} = (P) + (Q) - (P + Q) - (0_E)$.

Double and add algorithms

- If $D = div f_{\ell,P} = \ell(P) - (\ell P) - (\ell - 1)(0)$, the naïve Miller algorithm to get $f_{\ell,P}$ computes P, $P+P$, $P+P+P$, ..., ℓP.
- But to compute ℓP directly we can use a double and add algorithm;
- We can do the same in Miller's algorithm: decompose $D = D_1 + 2D_2 + 4D_3 + \cdots + 2^n D_n$, and do double and add.

Proposition

$$f_{\ell_1+\ell_2,P} = f_{\ell_1,P} \cdot f_{\ell_2,P} \cdot \mu_{\ell_1 P,\ell_2 P}$$

- Double and add algorithm:
- Initialisation: $T = P, f = 1 = f_{1,P}$.
- Double: $f := f^2 \mu_{Q,Q}$, $Q := Q + Q$;
- Add if $b_i = 1$: $f := f \mu_{Q,P}$, $Q := Q + P$.

Evaluating a function at a divisor

- If $f \in k(C)$ and $D = \sum n_i(P_i)$, $f(C) = \prod f(P_i)^{n_i}$.
- This is well defined is D and f have disjoint support. (Otherwise we may still define $f(D)$ by normalizing f along uniformisers on the intersection of the supports).
- If $\deg D = 0$, $f(D) = (\lambda f)(D)$. So if E is a principal divisor, $f_E(D)$ is well defined and does not depend on a choice of normalisation of f_E.

Theorem (Weil's reciprocity)

Let D_1, D_2 be two principal divisors (with disjoint support).

$$f_{D_1}(D_2) = f_{D_2}(D_1).$$

Remark

- *If D_1 and D_2 have non disjoint support, we have $f_{D_1}(D_2) = \epsilon f_{D_2}(D_1)$ with $\epsilon = \pm 1 = (-1)^{\sum_P v_P(D_1) v_P(D_2)}$.*
- *If $C = \mathbb{P}^1$, $f, g \in k[x]$, $div f(div g) = \operatorname{Res}(f,g)$, so Weil's reciprocity comes from $\operatorname{Res}(f,g) = (-1)^{\deg f \deg g} \operatorname{Res}(g,f)$ (f, g have a common pole at ∞).*

Evaluating $f_{\ell,P}(Q)$

- $f_{\ell,P}((Q)-(0)) = f_{\ell,P}(Q)$ by our choice of normalisation.
- Double and add algorithm:
- Initialisation: $T = P, f = 1$.
- Double: $\alpha = \frac{3x_T^2+a}{2y_T}$, $x_{2T} = \alpha^2 - 2x_T$, $y_{2T} = -y_T - \alpha(x_{2T} - x_T)$, $f := f^2 \frac{y_Q - y_T - \alpha(x_Q - x_T)}{x_Q + 2x_T - \alpha^2}$, $T := 2T$;
- Add if $b_i = 1$: $\alpha = \frac{y_T - y_P}{x_T - x_P}$, $x_{T+P} = \alpha^2 - x_T - x_P$, $y_{T+P} = -y_T - \alpha(x_{T+P} - x_T)$, $f := f \frac{y_Q - y_T - \alpha(x_Q - x_T)}{x_Q + x_P + x_T - \alpha^2}$, $T := T + P$;
- Warning, at the last step $f := f(x_Q - x_T)$.