Elliptic curve V

Divisors and Miller's algorithm

I) Motivations:

Goal: compute pairings

The Weil pairing $e_{W,\ell}: E[\ell] \times E[\ell] \longrightarrow \mu_\ell$

$$P, Q \longrightarrow \frac{f_{\ell,P}(Q)}{f_{\ell,Q}(P)}$$

$f_{\ell,P}$ is the unique rational function in $k(E)$ with a zero of order ℓ at P and a pole of order ℓ at O_E, which is normalized at infinity

Goal: construct $f_{\ell,P}$. More generally: given poles and zeroes with multiplicities, construct a function with these multiplicities if it exists.

II) Divisors on curves:

Let $\mathcal{C}/k$ be a smooth projective curve. Recall that for each $P \in \mathcal{C}(\bar{k})$, there is a corresponding ~~simulation~~ valuation v_P on $k(\mathcal{C})$.
If $f \in k(\mathcal{C})$ is a rational function on $\mathcal{C}$.
Define $\operatorname{div}(f) = \sum_{P \in \mathcal{C}(\bar{k})} v_P(f)(P)$ a formal sum of points.

Example: $f = \frac{X^2(X-2)}{X-1}$ in $k(\mathbb{P}^1) = k(X)$

$\operatorname{div}(f) = 2(x=0) + 1(x=2) - 1(x=1) - 2(x=\infty)$

Lemma: if $f \in k(\mathcal{C})$, it only has a finite number of poles and zeroes, so $\operatorname{div}(f)$ only involve a finite normal sum.

Definition: A divisor D on $\mathcal{C}$ is a finite formal sum of points:
$D = \sum_{P \in \mathcal{C}(k)} m_P (P)$, where $m_P = 0$ for all but a finite number of points.

Definition: $\deg(D) = \sum m_P$

Theorem: 1) If $f \in k(\mathcal{C})$, $\deg \operatorname{div}(f) = 0$
2) If $\operatorname{div}(f) = 0$ ie if f has no pole or zeroes, the f is constant: $f = \alpha$, $\alpha \in k^*$

Corollary: if $\operatorname{div}(f) = \operatorname{div} g$ then $\operatorname{div}(f/g) = \operatorname{div}(f) - \operatorname{div}(g) = 0$
then $\boxed{f = \alpha g, \ \alpha \in k^*}$

Definition: * D is linearly equivalent to 0 if $D = \operatorname{div}(f)$
* D and D' are linearly equivalent if $D - D'$ is linearly equivalent to 0, ie $D = D' + \operatorname{div}(f)$
* $\operatorname{Pic}^0(\mathcal{C}) = \{$Divisors of $\mathcal{C}$ of degree $0\}$ modulo linear equivalence
(this is a group since we can sum divisors and this is compatible with equivalence)

III) Divisors on $\mathbb{P}^1$:

Let $f \in k(\mathbb{P}^1) = k(x)$. Over $\bar{k}$, $f = \dfrac{\prod (x - \alpha_i)^{m_i}}{\prod (x - \beta_i)^{n_i}} \times \gamma$

$\deg f = \sum m_i - \sum n_i$

$$\boxed{\operatorname{div}(f) = \sum m_i (\alpha_i) - \sum n_i (\beta_i) - \deg f (\infty)}$$

$\deg \operatorname{div}(f) = 0$

* If f has no poles and zeroes, over k its denominator and numerator have degree 0, so $f = \frac{\alpha}{\beta} = \gamma \in k^*$

* Let $D = \sum n_i (\alpha_i)$ with $\deg(D) = 0$, so $\sum n_i = 0$. Does D come from a rational function?

$$D = \sum_{\alpha_i \neq 0} n_i (\alpha_i) - \left(\sum n_i\right)(\infty)$$

$$\boxed{f_D = \prod (X - \alpha_i)^{n_i}}$$

$\operatorname{div}(f_D) = D$

There is no obstruction ie $\operatorname{Pic}^0(\mathbb{P}^1) = 0$

* Normalisation : we say that f_D is normalised (at infinity) if

$-\operatorname{div}(f_D) = D$

$-f_D = \frac{\sum a_i x^i}{\sum b_i x^i}$ then $\frac{a_n}{b_m} = 1$

The quotient of the coefficients of the highest degree is equal to 1.

Remember that $\Pi_\infty = \frac{1}{X}$ is a uniformiser at ∞.

If $f \in k(X)$, $\frac{f}{\Pi_\infty^{v_\infty(f)}}$ is well defined at ∞

$$\boxed{f \text{ is normalised at } \infty \iff \left(\frac{f}{\Pi_\infty^{v_\infty(f)}}\right)(\infty) = 1}$$

IV) Divisors on E:

Lemma: If $f \in k(E)$, $\deg \operatorname{div} f = 0$

Proof: If $\operatorname{div} f = \sum n_P (P)$
$\operatorname{div} f = \sum n_P (-P)$
$2 \deg \operatorname{div} f = \deg \operatorname{div} f + \deg \operatorname{div} f = \deg \operatorname{div}(ff) = \deg \operatorname{div}(Nf)$
$Nf \in k(x)$
$\operatorname{div} Nf = \sum_{P \text{ not weierstrass}} v_P(Nf)(P) + \sum_{P \text{ weierstrass}} v_P(Nf)(P)$

* If P not Weierstrass, $v_P(Nf) = v_{x=x_P}(Nf)$ because $x - x_P$ is a uniformizer
But $-P$ has the same x_P:
$v_P(Nf) + v_{-P}(Nf) = 2 v_{x=x_P}(Nf)$

* If $P = (x_P, 0)$ is a Weierstrass, it is the only point with x-coordinate x_P but y is a uniformizer, and $v_P(x - x_P) = 2$
So $v_P(Nf) = 2 v_{x=x_P} Nf$.

* Conclusion: $\deg \operatorname{div}_E Nf = 2 \deg \operatorname{div}_{P_1} Nf = 0$

Theorem: Let $D = \sum n_P (P) \in \operatorname{Div}^0(E)$. Then $D \sim 0$ if and only if $\sum n_P P = 0$ in $E(\bar{k})$

Corollary: Let $\Sigma_D = \sum n_P P \in E(\bar{k})$, $D \sim (\Sigma_D) - (O_E)$

Proof: $D - (\Sigma_D) + (O_E)$ has degree 0, and $\sum n_P P - \Sigma_D = O_E$ by definition

Reformulation: $\operatorname{Pic}^0(E) \simeq E(\bar{k})$: "algebraic interpretation of the group law"

I) Miller's algorithm:

Goal: Given D such that $\deg D = 0$ and $\sum_D = O_E$
construct f_D « normalized at infinity » such that $\operatorname{div} f_D = D$

* $\Pi_{O_E} = \frac{X}{Y}$ is a uniformizer at O_E
f_D is normalized at infinity if $\left(\frac{f_D}{\Pi_{O_E}^{v_{O_E}(f_D)}}\right)(O_E) = 1$

if and only if α, β are the coeffs of highest degree of the numerator and denominator, $\boxed{\frac{\alpha}{\beta} = 1}$

* Fundamental case: $D = (P) + (Q) - (P+Q) - (O_E)$
Definition: $\nu_{P,Q}$ is the normalized function with divisor $(P)+(Q)-(P+Q)-(O_E)$

* Reduction: $D = (P_1) + (P_2) + (P_3) + \cdots$
$D = \operatorname{div} \nu_{P_1,P_2} + (P_1+P_2) + (O_E) + (P_3) + \cdots = \operatorname{div} \nu_{P_1,P_2} + \operatorname{div} \nu_{P_1+P_2,P_3} + (P_1+P_2+P_3) + \cdots$

Note: $\operatorname{div} \nu_{P,-P} = (P) + (-P) - 2(O_E)$
So $-(P) + (O_E) \sim (-P) - (O_E)$

Example: $D = 5(P) - 5(O_E)$ where $P \in E[5]$
$D = \operatorname{div} \nu_{P,P} + (2P) + (3P) - 4(O_E) = \operatorname{div} \nu_{P,P} + \operatorname{div} \nu_{P,2P} + (3P) + 2(P) - 3(O_E)$
$= \operatorname{div} \nu_{P,P} + \operatorname{div} \nu_{P,2P} + \operatorname{div} \nu_{P,3P} + (4P) + (P) - 2(O_E)$

$= \operatorname{div} \nu_{P,P} + \operatorname{div} \nu_{P,2P} + \operatorname{div} \nu_{P,3P} + \operatorname{div} \nu_{P,4P} + (5P) - (O_E)$
$\to 0$ as $P \in E[5]$

$\Rightarrow f_D = \nu_{P,P}\, \nu_{P,2P}\, \nu_{P,3P}\, \nu_{P,4P}$ is normalized because the $\nu_{P,Q}$ are

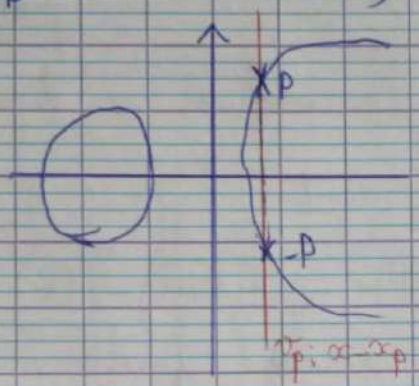
* More generally, using the $\nu_{P,Q}$ we can always reduce D to $\sum (P) - (O_E)$

* Conversely, if $D=(P)-(O_E)$ were ~ 0 with $P \neq O_E$, then the function f_D would induce an isomorphism $f_D: E \xrightarrow{\sim} \mathbb{P}^1$ but this is impossible since they don't have the same genus.

* Constructing $\mu_{P,Q}$

a) $Q=-P$ / $\mu_{P,-P}$

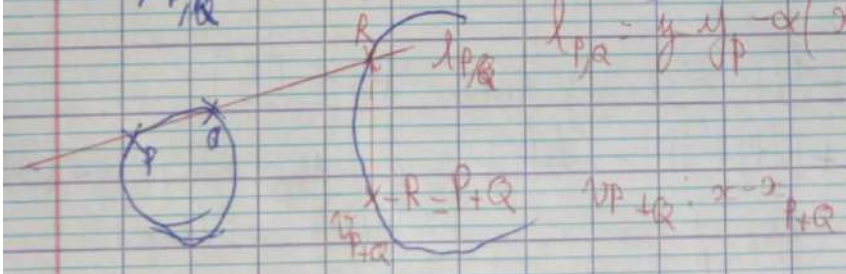
$\operatorname{div} \mu_{P,-P} = (P)+(-P)-2(O_E)$



Lemma: $\mu_{P,-P} = x - x_P$

b) $Q \neq -P$

$\operatorname{div} \mu_{P,Q} = (P)+(Q)-(P+Q)-(O_E)$



$\operatorname{div} l_{P,Q} = (P)+(Q)+(R)-3(O_E)$

$\Rightarrow f_D = \mu_{P,1P}\,\mu_{P,2P}\,\mu_{P,3P}\,\mu_{P,4P}$

$\operatorname{div} v_{P+Q} = (P+Q)+(R)-2(\infty)$

$$\mu_{P,Q} = \frac{l_{P,Q}}{v_{P+Q}} = \frac{y - y_P - \alpha(x - x_P)}{x - x_{P+Q}}$$ it is normalised

VI) Miller's algorithm:

Let $P \in E[l]$, $D = l(P) - l(O_E) \sim 0$

Definition: $f_{l,P}$ the normalized function with this divisor

Reduction: $(P)+(P) \sim (2P) + (O_E)$ via $\mu_{P,P}$
$(2P)+(P) \sim (3P) + (O_E)$ via $\mu_{2P,P}$
$(3P)+(P) \sim (4P) + (O_E)$ via $\mu_{3P,P}$

$\Delta \Longrightarrow O(l)$ Too slow

Solution: use the double and add method.

Informally: $(P)+(P) \sim (2P)+(O_E)$
$(2P)+(2P) \sim (4P)+(O_E)$
$(4P)+(4P) \sim (8P)+(O_E)$

Rigourously: For any P, define $f_{l,P}$ such that it is normalised and $\operatorname{div} f_{l,P} = l(P) - (lP) - (l-1)(O_E)$

Exercise: a) $f_{l,P}$ exists
b) If $P \in E[l]$ then is the same function as before
c) $f_{l_1+l_2,P} = f_{l_1,P} f_{l_2,P} \mu_{l_1P,l_2P}$

Hint: check that the divisors are the same $\Rightarrow$ the functions are equal since they are normalised.

Corollary: Double and add

Double: $f_{2l,P} = f_{l,P}^2 \, \mu_{l_P, l_P}$

Add: $f_{l+1,P} = f_{l,P} \, \mu_{l_P, P}$

Remark: $f_{0,P} = f_{1,P} = 1$

Millers algo: Input: $l, P \in E[l]$, $Q \in E$

Output: $f_{l,P}(Q)$

- Write $l = \sum b_i 2^i$ $T = O$ $f = 1$
- For each bits b_i from left to right
  - Double: $f = f^2 \times \mu_{T,T}(Q)$, $T = 2T$
  - If $b_i = 1$ Add: $f = f \times \mu_{T,P}(Q)$, $T = T + P$

Return f.