Weil Pairing - study

arnaucube

August 2022

Abstract

Notes taken from Matan Prasma math seminars and also while reading about Bilinear Pairings. Usually while reading papers and books I take handwritten notes, this document contains some of them re-written to $LaTeX$.

The notes are not complete, don't include all the steps neither all the proofs. I use these notes to revisit the concepts after some time of reading the topic.

Contents

1 Rational functions

Let $E/\mathbb{k}$ be an elliptic curve defined by: $y^2 = x^3 + Ax + B$.

set of polynomials over E: $\mathbb{k}[E] := \mathbb{k}[x, y]/(y^2 - x^3 - Ax - B = 0)$
we can replace y^2 in the polynomial $f \in \mathbb{k}[E]$ with $x^3 + Ax + B$

canonical form: $f(x, y) = v(x) + yw(x)$ for $v, w \in \mathbb{k}[x]$

conjugate: $\overline{f} = v(x) - yw(x)$

norm: $N_f = f \cdot \overline{f} = v(x)^2 - y^2 w(x)^2 = v(x)^2 - (x^3 + Ax + B)w(x)^2 \in \mathbb{k}[x] \subset \mathbb{k}[E]$

we can see that $N_{fg} = N_f \cdot N_g$

set of rational functions over E: $\mathbb{k}(E) := \mathbb{k}[E] \times \mathbb{k}[E] / \sim$

For $r \in \mathbb{k}(E)$ and a finite point $P \in E(\mathbb{k})$, r is *finite* at P iff

$$\exists\ r = \frac{f}{g} \text{ with } f, g \in \mathbb{k}[E],\ s.t.\ g(P) \neq 0$$

We define $r(P) = \frac{f(P)}{g(P)}$. Otherwise, $r(P) = \infty$.

Remark: $r = \frac{f}{g} \in \mathbb{k}(E)$, $r = \frac{f}{g} = \frac{f \cdot \overline{g}}{g \cdot \overline{g}} = \frac{f\overline{g}}{N_g}$, thus

$$r(x, y) = \frac{(f\overline{g})(x, y)}{N_g(x, y)} = \underbrace{\frac{v(x)}{N_g(x)} + y\frac{w(x)}{N_g(x)}}_{\text{canonical form of } r(x,y)}$$

degree of f: Let $f \in \mathbb{k}[E]$, in canonical form: $f(x, y) = v(x) + yw(x)$,

$$deg(f) := max\{2 \cdot deg_x(v), 3 + 2 \cdot deg_x(w)\}$$

For $f, g \in \mathbb{k}[E]$:

i. $deg(f) = deg_x(N_f)$

ii. $deg(f \cdot g) = deg(f) + deg(g)$

Def 1.1. Let $r = \frac{f}{g} \in \mathbb{k}(E)$

i. if $deg(f) < deg(g)$: $r(0) = 0$

ii. if $deg(f) > deg(g)$: r is not finite at 0

iii. if $deg(f) = deg(g)$ with $deg(f)$ even:
f's canonical form leading terms ax^d
g's canonical form leading terms bx^d
$a, b \in \mathbb{k}^\times$, $d = \frac{deg(f)}{2}$, set $r(0) = \frac{a}{b}$

iv. if $deg(f) = deg(g)$ with $deg(f)$ odd
f's canonical form leading terms ax^d
g's canonical form leading terms bx^d
$a, b \in \mathbb{k}^\times$, $deg(f) = deg(g) = 3 + 2d$, set $r(0) = \frac{a}{b}$

1.1 Zeros, poles, uniformizers and multiplicities

$r \in \mathbb{k}(E)$ has a *zero* in $P \in E$ if $r(P) = 0$
$r \in \mathbb{k}(E)$ has a *pole* in $P \in E$ if $r(P)$ is not finite.

uniformizer: Let $P \in E$, uniformizer: rational function $u \in \Bbbk(E)$ with $u(P) = 0$ if $\forall r \in \Bbbk(E) \setminus \{0\},\ \exists d \in \mathbb{Z},\ s \in \Bbbk(E)$ finite at P with $s(P) \neq 0$ s.t.

$$r = u^d \cdot s$$

order: Let $P \in E(\Bbbk)$, let $u \in \Bbbk(E)$ be a uniformizer at P. For $r \in \Bbbk(E) \setminus \{0\}$ being a rational function with $r = u^d \cdot s$ with $s(P) \neq 0, \infty$, we say that r has *order* d at P ($ord_P(r) = d$).

multiplicity: *multiplicity of a zero* of r is the order of r at that point, *multiplicity of a pole* of r is the order of r at that point.

if $P \in E(\Bbbk)$ is neither a zero or pole of r, then $ord_P(r) = 0$ $(= d,\ r = u^0 s)$.

Multiplicities, from the book "Elliptic Tales" (p.69), to provide intuition

Factorization into *linear factors*: $p(x) = c \cdot (x - a_1) \cdots (x - a_d)$

d: degree of $p(x)$, $a_i \in \Bbbk$

Solutions to $p(x) = 0$ are $x = a_1, \ldots, a_d$ (some a_i can be repeated)

eg.: $p(x) = (x-1)(x-1)(x-3)$, solutions to $p(x) = 0 :\ 1, 1, 3$

$x = 1$ is a solution to $p(x) = 0$ of *multiplicity* 2.

The total number of solutions (counted with multiplicity) is d, the degree of the polynomial whose roots we are finding.

2 Divisors

Def 2.1. Divisor

$$D = \sum_{P \in E(\Bbbk)} n_p \cdot [P]$$

Def 2.2. Degree & Sum

$$deg(D) = \sum_{P \in E(\Bbbk)} n_p$$

$$sum(D) = \sum_{P \in E(\Bbbk)} n_p \cdot P$$

The set of all divisors on E forms a group: for $D = \sum_{P \in E(\Bbbk)} n_P[P]$ and $D' = \sum_{P \in E(\Bbbk)} m_P[P]$,

$$D + D' = \sum_{P \in E(\Bbbk)} (n_P + m_P)[P]$$

Def 2.3. Associated divisor

$$div(r) = \sum_{P \in E(\Bbbk)} ord_P(r)[P]$$

Observe that

$div(rs) = div(r) + div(s)$

$div(\frac{r}{s}) = div(r) - div(s)$

Observe that

$$\sum_{P \in E(\Bbbk)} ord_P(r) \cdot P = 0$$

Def 2.4. Support of a divisor

$$\sum_P n_P[P],\ \forall P \in E(\Bbbk) \text{ s.t. } n_P \neq 0$$

Def 2.5. Principal divisor iff

$$deg(D) = 0$$

$$sum(D) = 0$$

$D \sim D'$ iff $D - D'$ is principal.

Def 2.6. Evaluation of a rational function (function r evaluated at D)

$$r(D) = \prod r(P)^{n_p}$$

3 Weil reciprocity

Thm 3.1. (Weil reciprocity) Let $E/\Bbbk$ be an e.c. over an algebraically closed field. If $r,\ s \in \Bbbk \backslash \{0\}$ are rational functions whose divisors have disjoint support, then

$$r(div(s)) = s(div(r))$$

Proof. (todo)

Example

$$p(x) = x^2 - 1,\ q(x) = \frac{x}{x-2}$$

$$div(p) = 1 \cdot [1] + 1 \cdot [-1] - 2 \cdot [\infty]$$

$$div(q) = 1 \cdot [0] - 1 \cdot [2]$$

(they have disjoint support)

$$p(div(q)) = p(0)^1 \cdot p(2)^{-1} = (0^2 - 1)^1 \cdot (2^2 - 1)^{-1} = \frac{-1}{3}$$

$$q(div(p)) = q(1)^1 \cdot q(-1)^1 - q(\infty)^2$$

$$= (\frac{1}{1-2})^1 \cdot (\frac{-1}{-1-2})^1 \cdot (\frac{\infty}{\infty - 2})^2 = \frac{-1}{3}$$

so, $p(div(q)) = q(div(p))$.

4 Generic Weil Pairing

Let $E(\mathbb{k})$, with $\mathbb{k}$ of char p, n s.t. $p \nmid n$.

$\mathbb{k}$ large enough: $E(\mathbb{k})[n] = E(\overline{\mathbb{k}}) = \mathbb{Z}_n \oplus \mathbb{Z}_n$ (with n^2 elements).

For $P, Q \in E[n]$,

$$D_P \sim [P] - [0]$$
$$D_Q \sim [Q] - [0]$$

We need them to have disjoint support:

$$D_P \sim [P] - [0]$$
$$D'_Q \sim [Q+T] - [T]$$

$$\Delta D = D_Q - D'_Q = [Q] - [0] - [Q+T] + [T]$$

Note that nD_P and nD_Q are principal. Proof:

$$nD_P = n[P] - n[O]$$
$$deg(nD_P) = n - n = 0$$
$$sum(nD_P) = nP - nO = 0$$

($nP = 0$ bcs. P is n-torsion)

Since nD_P, nD_Q are principal, we know that f_P, f_Q exist.

Take

$$f_P : div(f_P) = nD_P$$
$$f_Q : div(f_Q) = nD_Q$$

We define

$$e_n(P,Q) = \frac{f_P(D_Q)}{f_Q(D_P)}$$

Remind: evaluation of a rational function over a divisor D:

$$D = \sum n_P[P]$$
$$r(D) = \prod r(P)^{n_P}$$

If $D_P = [P+S] - [S]$, $\;D_Q = [Q-T] - [T]$ what is $e_n(P,Q)$?

$$f_P(D_Q) = f_P(Q+T)^1 \cdot f_P(T)^{-1}$$
$$f_Q(D_P) = f_Q(P+S)^1 \cdot f_Q(S)^{-1}$$

$$e_n(P,Q) = \frac{f_P(Q+T)}{f_P(T)} / \frac{f_Q(P+S)}{f_Q(S)}$$

with $S \neq \{O, P, -Q, P-Q\}$.

5 Properties

i. $e_n(P,Q)^n = 1 \; \forall P, Q \in E[n]$
(⇒ $e_n(P,Q)$ is a n^{th} root of unity)

ii. Bilinearity

$$e_n(P_1 + P_2, Q) = e_n(P_1, Q) \cdot e_n(P_2, Q)$$

$$e_n(P, Q_1 + Q_2) = e_n(P, Q_1) \cdot e_n(P, Q_2)$$

proof: recall that $e_n(P,Q) = \frac{g(S+P)}{g(S)}$, then,

$$e_n(P_1, Q) \cdot e_n(P_2, Q) = \frac{g(P_1 + S)}{g(S)} \cdot \frac{g(P_2 + P_1 + S)}{g(P_1 + S)}$$

(replace S by $S + P_1$)

$$= \frac{g(P_2 + P_1 + S)}{g(S)} = e_n(P_1 + P_2, Q)$$

iii. Alternating

$$e_n(P,P) = 1 \; \forall P \in E[n]$$

iv. Nondegenerate

$$\text{if } e_n(P,Q) = 1 \; \forall Q \in E[n], \text{ then } P = 0$$

6 Exercises

An Introduction to Mathematical Cryptography, 2nd Edition - Section 6.8. Bilinear pairings on elliptic curves

6.29. $div(R(x) \cdot S(x)) = div(R(x)) + div(S(x))$, where $R(x), S(x)$ are rational functions.
proof:
Norm of f: $N_f = f \cdot \overline{f}$, and we know that $N_{fg} = N_f \cdot N_g \; \forall \; \Bbbk[E]$,
then

$$deg(f) = deg_x(N_f)$$

and

$$deg(f \cdot g) = deg(f) + deg(g)$$

Proof:

$$deg(f \cdot g) = deg_x(N_{fg}) = deg_x(N_f \cdot N_g)$$

$$= deg_x(N_f) + deg_x(N_g) = deg(f) + deg(g)$$

So, $\forall P \in E(\Bbbk),\; ord_P(rs) = ord_P(r) + ord_P(s)$.
As $div(r) = \sum_{P \in E(\Bbbk)} ord_P(r)[P]$, $div(s) = \sum ord_P(s)[P]$.

So,

$$div(rs) = \sum ord_P(rs)[P]$$

$$= \sum ord_P(r)[P] + \sum ord_P(s)[P] = div(r) + div(s)$$

6.31.

$$e_m(P,Q) = e_m(Q,P)^{-1} \forall P,Q \in E[m]$$

Proof: We know that $e_m(P,P) = 1$, so:

$$1 = e_m(P+Q, P+Q) = e_m(P,P) \cdot e_m(P,Q) \cdot e_m(Q,P) \cdot e_m(Q,Q)$$

and we know that $e_m(P,P) = 1$, then we have:

$$1 = e_m(P,Q) \cdot e_m(Q,P)$$

$$\implies e_m(P,Q) = e_m(Q,P)^{-1}$$