Goal: To define Weil Pairing and discuss its properties

Recall: C/K

Divisor is a formal sum $\sum_{P \in C} n_P P$ $\quad P \in C$

Principal divisor: i.e divisor of the form $\mathrm{div}(f)$ for some $f \in \bar{K}(C)$

$$\left\{ \begin{array}{c} \text{Set of all} \\ \text{principal divisors} \end{array} \right\} \subseteq \left\{ \begin{array}{c} \text{Set of all degree zero} \\ \text{divisors} \end{array} \right\}$$

$$\neq \text{if}$$

$$\left\{ \begin{array}{c} \text{Set of all} \\ \text{divisors} \end{array} \right\}$$

Let E be an elliptic curve defined over K.

Define: $\mathrm{Pic}^0(E) = \dfrac{\left\{ \begin{array}{c} \text{Group of all degree 0} \\ \text{divisors on } E \end{array} \right\}}{\left\{ \begin{array}{c} \text{Group of all Principal} \\ \text{divisors} \end{array} \right\}}$

Thm: $\mathrm{Pic}^0(E) \cong E$

$D \in \mathrm{Pic}^0(E)$

$D \sim (P) - (\mathcal{O})$ $\left(\exists\ P \in E \text{ s.t } D \sim (P) - (\mathcal{O})\right)$

($\mathcal{O}$: point at infinity)

$\sigma : D \longmapsto P$

Observation: D degree 0

D is principal $\iff \sum [n_p] P = \mathcal{O}$

$D = \sum n_p P$

D is principal $\iff D \sim 0$

degree 0

$\iff \sigma(D) = \mathcal{O}$

$\iff \sigma\left(\sum n_p P\right) = \mathcal{O}$

$\iff \sigma\left(\sum n_p P - \left(\sum n_p\right)\mathcal{O}\right) = \mathcal{O}$

$\iff \sigma\left(\sum n_p (P - \mathcal{O})\right) = \mathcal{O}$

$\iff \sum n_p \sigma(P - \mathcal{O}) = \mathcal{O}$

$$\iff \sum m_P P = \mathcal{O}$$

Setup: E/K Elliptic curve defined over K

N N is coprime to $\text{char}(K)$

$$E[N] = \{ P \in E(\bar{K}) \mid NP = \mathcal{O} \}$$

↳ N-torsion points

Weil Pairing is a function $e_N : E[N] \times E[N] \to \mu_N$

Recipe: Let $Q \in E[N]$.

$$\text{div}(f) = NQ - N\mathcal{O}$$

($NQ - N\mathcal{O}$ is principal, hence there exists a function f s.t $\text{div}(f) = NQ - N\mathcal{O}$)

Let Q' be s.t $NQ' = Q$.

Using Q' we will construct another divisor.

$\sum_{R \in E[N]} (Q'+R) - (R)$, this is a degree 0 divisor

$$\#E[N] = N^2$$

$$N^2 Q' = N(NQ') = NQ = \mathcal{O}$$

→ this is also a principal divisor.

So there exists a function g s.t

$$\text{div}(g) = \sum_{R \in E[N]} (Q'+R) - R$$

Some more observations

$$\text{div}(g^N) = N \,\text{div}(g)$$

$$= \sum_{R \in E[N]} N(Q'+R) - N(R)$$

$$[N] : E \to E$$

$$P \mapsto NP$$

$$\operatorname{div}(f \circ [N])$$

$$f \circ [N](X) = f(NX)$$

$$\operatorname{div}(f) = NQ - N\mathcal{O}$$

$$NX = Q$$

$$[N(Q' + R) = NQ' + NR = Q]$$

$$\operatorname{div}(f \circ [N]) = N\left(\sum_{R \in E[N]} (Q' + R) - (R)\right)$$

$$\Rightarrow \quad \operatorname{div}(f \circ [N]) = \operatorname{div}(g^N)$$

$$\Rightarrow \quad f \circ [N] = g^N \quad (\text{up to a constant})$$

By adjusting f with this constant, assume

$$f_Q \circ [N] = g_Q^N$$

Let $P \in E[N]$, then for any $X \in E$

$$g_Q(X+P)^N = f_Q \circ [N](X+P)$$

$$= f_Q(NX + NP)$$

$$= f_Q(NX)$$

$$= f_Q \circ [N](X) = g_Q^N(X)$$

$$\Rightarrow \left(\frac{g_Q(X+P)}{g_Q(X)}\right)^N = 1$$

$\Rightarrow$ $\downarrow$ is some N-th root of unity.

This does not depend on choice of X.

$$E \to \mathbb{P}^1$$

$$X \longmapsto \frac{g_Q(X+P)}{g_Q(X)} \quad \text{(morphism)}$$

Weil Pairing $e_N : E[N] \times E[N] \to \mu_N$

$$(P, Q) \longmapsto \frac{g_Q(X+P)}{g_Q(X)}$$

Properties of Weil Pairing

1) Bilinear in both variables

$$e_N(P_1+P_2, Q) = e_N(P_1, Q)\, e_N(P_2, Q)$$

$$e_N(P, Q_1+Q_2) = e_N(P, Q_1)\, e_N(P, Q_2)$$

2) Alternating

$$e_N(P, P) = 1$$

$$\Rightarrow e_N(P, Q) = e_N(Q, P)^{-1}$$

3) Non-degenerate

If $e_N(P, Q) = 1$ for all $Q \in E[N]$

$$\Rightarrow P = \mathcal{O}$$

If $e_N(P, Q) = 1$ for all $P \in E[N]$

$$\Rightarrow Q = \mathcal{O}$$

4) Galois-invariant

$$\sigma \in Gal(\overline{K}/K)$$

$$\sigma(e_N(P,Q)) = e_N(\sigma P, \sigma Q)$$

5) Compatibility among e_N's

If $S \in E[NN']$

$P \in E[N] \subseteq E[NN']$

$$e_{NN'}(S,P) = e_N(N'S, P)$$

Next time: (1) See a proof of these properties

(2) Explicit applications in cryptography

Reference: Silverman's Arithmetic of elliptic curves / Ch.3 Weil Pairing

Proof of properties:

1) Bilinear

$$e_N(P_1+P_2, Q) = e_N(P_1, Q)\, e_N(P_2, Q)$$

$$e_N(P, Q_1+Q_2) = e_N(P, Q_1)\, e_N(P, Q_2)$$

Pf: Want to show that

$$e_N(P_1+P_2, Q) = e_N(P_1, Q)\, e_N(P_2, Q)$$

$$e_N(P_1+P_2, Q) = \frac{g_Q(X+(P_1+P_2))}{g_Q(X)}$$

$$= \frac{g_Q(X+(P_1+P_2))\; g_Q(X+P_1)}{g_Q(X)\; g_Q(X+P_1)}$$

$$= \frac{g_Q(X+(P_1+P_2))}{g_Q(X+P_1)} \cdot \frac{g_Q(X+P_1)}{g_Q(X)}$$

$$= e_N(P_2, Q)\, e_N(P_1, Q)$$

2) Alternating

$$e_N(P,P) = 1$$

&

$$e_N(P,Q) = e_N(Q,P)^{-1}$$

It suffices to show that $e_N(P,P)=1$

$$e_N(P+Q, P+Q) = 1 \quad \forall P,Q \in E[N]$$

$$\| $$

$$e_N(P+Q, P)\, e_N(P+Q, Q) = 1$$

$$\| \qquad\qquad \| $$

$$e_N(P,P)\, e_N(Q,P)\, e_N(P,Q)\, e_N(Q,Q) = 1$$

$$\| \qquad\qquad\qquad\qquad \| $$

$$1 \qquad\qquad\qquad\qquad 1$$

$$e_N(Q,P)\, e_N(P,Q) = 1$$

$$\Rightarrow \quad e_N(P,Q) = e_N(Q,P)^{-1}$$

Let us show that $e_N(Q,Q) = 1 \ \forall Q \in E[N]$

$$e_N(Q,Q) = g_Q(X+Q) / g_Q(X)$$

Translation map

$$\tau_s : E \longrightarrow E$$

$$x \longmapsto x + s$$

$$\operatorname{div}\left(\prod_{i=0}^{N-1} f \circ \tau_{iQ}\right)$$

[Recall $\operatorname{div}(f) = NQ - N\mathcal{O}$]

$$\operatorname{div}(g_1 g_2) = \operatorname{div}(g_1) + \operatorname{div}(g_2)$$

$$\operatorname{div}(f \circ \tau_{iQ}) = N(Q - iQ) - N(-iQ)$$

$$f(x) = 0$$

$$f \circ \tau_{iQ}(Y) = 0$$

$$f(iQ + Y) = 0$$

$$Y = x - iQ$$

$$\operatorname{div}\left(\prod_{i=0}^{N-1} f \circ \tau_{iQ}\right) = N\left(\sum_{i=0}^{N-1} (Q - iQ) - (-iQ)\right)$$

(Points; Points; Coefficients; Coeffs)

$$= 0$$

$N = 3$

$$3\left(Q - \cancel{0} + \cancel{0} - \cancel{(-Q)} + \cancel{(-Q)} - (-2Q)\right)$$

$3Q = 0$

$2Q = -Q$

$-2Q = Q$

$$3(Q - Q) = 0$$

So, $\prod_{i=0}^{N-1} f \circ T_{[i]Q}$ is constant

Now let us choose a point Q' such that $NQ' = Q$. (Recall $g^N = f$)

$$\left(\prod_{i=0}^{N-1} g \circ T_{iQ'}\right)^N = \prod_{i=0}^{N-1} f \circ T_{iQ}$$

$$= \text{Constant}$$

$$\Rightarrow \prod_{i=0}^{N-1} g \circ T_{iQ'} \text{ is also constant}$$

$$\prod_{i=0}^{N-1} g \circ T_{iQ'}(x) = \prod_{i=0}^{N-1} g(x + iQ')$$

$$= \prod_{i=0}^{N-1} g(x+Q'+iQ')$$

$$= \prod_{i=0}^{N-1} g(x+(i+1)Q')$$

After cancellations

$$g(x) = g(x+NQ')$$

$$g(x) = g(x+Q)$$

$$e_N(Q,Q) = \frac{g(x+Q)}{g(x)} = 1$$

(g is same as g_Q)

Question from chat

If $\text{char}(K) \neq 0 \not\Rightarrow K$ is finite.

Let R be any field.

$1+1+1+\cdots$ is never zero

$\underbrace{1+1+1+\cdots+1}_{m} = 0$

If $\text{char}(K) \neq 0 \Rightarrow \exists$ an m (smallest) s.t

$m1 = 0$

$\Rightarrow K$ is finite.

Example: $F_3[X] = \{$ Polynomials in single variable X with coeffs in $F_3\}$

$F_3(X) = \left\{ \frac{f}{g} \mid f, g \in F_3[X], g \neq 0 \right\}$

is infinite

$\{1, X, X^2, X^3, \ldots\} \subseteq F_3[X] \subseteq F_3(X)$

3) Non-degenerate

If $e_N(P,Q) = 1 \quad \forall P \in E[N]$ (fixed Q)

$\Rightarrow Q = \mathcal{O}$

$\Rightarrow g_Q(X+P) = g_Q(X) \quad \forall P \in E[N]$

There exists a function h such that

$g = h \circ [N]$

$[N] : E \to E$, $X \mapsto NX$

$(h \circ [N])^N = g^N$

$= f \circ [N]$

$\Rightarrow f = h^N$

$N \operatorname{div} h = \operatorname{div} f$

$= NQ - N\mathcal{O}$

$\operatorname{div} h = Q - \mathcal{O}$

$\downarrow$ principal divisor

$\Downarrow$

$Q = \mathcal{O}$

4) It respects Galois action

has errors please look at lecture 9

$\sigma \in Gal(\overline{K}/K)$ $\quad x^n - 1 = 0$

$$c_N(\sigma P, \sigma Q) = \frac{g_{\sigma Q}(x + \sigma P)}{g_{\sigma Q}(x)}$$

$$g_{\sigma Q}(x) = \sigma(g_Q(x))$$

$$= \frac{\sigma(g_Q(x + \sigma P))}{\sigma(g_Q(x))}$$

$$= \sigma\left(\frac{g_Q(x + \sigma P)}{g_Q(x)}\right)$$

$$= \sigma(e_N(\sigma P, Q))$$

↳ I will correct in next class.

5) Compatibility

If $S \in E[NN']$

$P \in E[N]$

$$e_{NN'}(S,P) = e_N(N'S,P)$$

$$\operatorname{div}(f^{N'}) = NN'(Q) - NN'(O)$$

$$\left(g \circ [N']\right)^{NN'} = \left(f \circ [NN']\right)^{N'}$$

$$e_{NN'}(S,P) = \frac{g \circ [N'](X+P)}{g \circ [N'](X)}$$

$$= \frac{g(Y+N'S)}{g(Y)}$$

$$= e_N(N'S,P)$$

Summary so far

$e_N : E[N] \times E[N] \to \mu_N$

↳ Weil Pairing

ECDLP Problem P, Q

$Q = rP$

How do we find r?

Okamoto

MOV attack

↓

Menezes

Vanstone

$E / \mathbb{F}_q$ $\quad q = p^r$

P, Q of order N $\quad p \nmid N$

Suppose $Q = rP$, but we don't know r.

① Compute $\# E(\mathbb{F}_{q^k}) = c$

N|C (by Lagrange's thm)

② Choose a $T \in E(\mathbb{F}_{q^k})$ such that $T \notin E(\mathbb{F}_q)$.

③ $S = \left(\frac{C}{N}\right) T$, If $S = \mathcal{O}$, then go back to ② and choose a different T.

④ $e_N(P, S)$

$e_N(P, S)^r = e_N(rP, S)$

$= e_N(Q, S)$

To find r, perform index calculus method to solve DLP in μ_N.