Sesquilinear pairings on elliptic curves (+ isogenies)

Katherine E. Stange (+ Joseph Macula)

ANTS, July 19th, 2024

Bilinear pairings

Let A, B, R be abelian groups. Let

$$\langle \cdot, \cdot \rangle : A \times B \to R$$

be linear in each factor.

Our interest: A and B groups of points on an elliptic curve.

Weil and Tate pairings

Weil pairing:

$$e_m : E(K)[m] \times E(K)[m] \to \mu_m$$

Tate pairing:

$$t_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$$

Implies fun cryptography. Example:

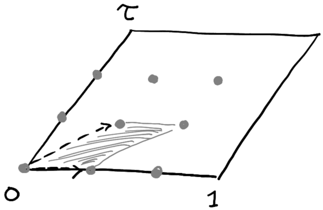
$$t_m([a]P, [b]Q)^c = t_m(P, Q)^{abc}.$$

Weil pairing over $\mathbb{C}$

Weil pairing over $\mathbb{C}$ (Galbraith has nice notes):

Let 1 and τ form a basis for Λ giving $E \cong \mathbb{C}/\Lambda$:

$$e_m\left(\frac{a+b\tau}{m}, \frac{c+d\tau}{m}\right) = e^{2\pi i \frac{ad-bc}{m}}.$$



Paths for homology of torus: $\gamma_1 : 0 \to 1$ and $\gamma_\tau : 0 \to \tau$.

$$(a\gamma_1 + b\gamma_\tau)\cdot(c\gamma_1 + d\gamma_\tau) = ad - bc.$$

Extensions

An extension

$$0 \longrightarrow \mathbb{G}_m \longrightarrow X \longrightarrow E \longrightarrow 0$$

is given by a factor set

$$f : E \times E \to \mathbb{G}_m$$

determining the group law on X via

$$(x,P)(y,Q) = (xyf(P,Q), P+Q).$$

Extensions

An extension

$$0 \longrightarrow K^* \longrightarrow X \longrightarrow E(K) \longrightarrow 0$$

is given by a factor set

$$f : E(K) \times E(K) \to K^*$$

determining the group law on X via

$$(x, P)(y, Q) = (xy\, f(P, Q), P + Q).$$

Monodromy

A group fact in E,

$$\sum P_i = \mathscr{O},$$

$$\Downarrow$$

a monodromy $\alpha \in K^*$:

$$\sum (x_i, P_i) = \left(\left(\prod x_i\right)\alpha, \mathscr{O}\right).$$

A biextension X ‘glues together’ many extensions:

X has action of K^* with quotient

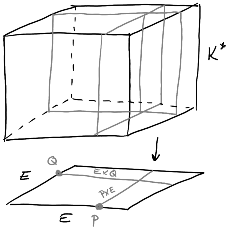
$$\pi : X \to E \times E$$

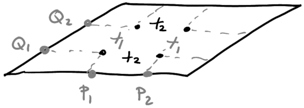
where fibres $X_{(P,Q)}$ are homogeneous spaces for K^*.

There are two compatible operations:

1. $+_1$ defined on $X_{\{P\}\times E}$;
2. $+_2$ defined on $X_{E\times\{Q\}}$.

Each $X_{\{P\}\times E}$
is an extension of E by K^* determined by P, and similarly.





The Poincaré biextension

In our case X is given by a biextension factor set

$$f : E \times E \times E \to K^*$$

so that f restricts to a factor set on $E \times E \times \{Q\}$ and $\{P\} \times E \times E$.

Let f be the rational function with divisor

$$C := m_{123}^*(\mathscr{O}) - m_{12}^*(\mathscr{O}) - m_{23}^*(\mathscr{O}) - m_{13}^*(\mathscr{O}) + m_1^*(\mathscr{O}) + m_2^*(\mathscr{O}) + m_3^*(\mathscr{O}).$$

Has an expression in terms of elliptic nets:

$$\frac{W(P+Q+R)W(P)W(Q)W(R)}{W(P+Q)W(Q+R)W(P+R)}.$$

Monodromy

Fixing Q in E, we have an extension $X_{E\times\{Q\}}$.

If $P \in E[m]$, then the group fact $mP = \mathcal{O}$ gives a monodromy on $X_{E\times\{Q\}}$.

This is the Tate pairing $t_m(P, Q)$.

The Weil pairing is the quotient

$$e_m(P, Q) = \frac{\text{monodromy of } mP = \mathcal{O} \text{ on } X_{E\times\{Q\}}}{\text{monodromy of } mQ = \mathcal{O} \text{ on } X_{\{P\}\times E}}$$

Weil and Tate pairings from monodromy

The extension $X_{E\times\{Q\}}$ has factor set

$$E\times E\to K^*,\quad (P,R)\mapsto f_{P,R}((Q)-(\mathscr{O}))$$

where

$$\mathrm{div}(f_{P,R})=(P+R)-(P)-(R)+(\mathscr{O}).$$

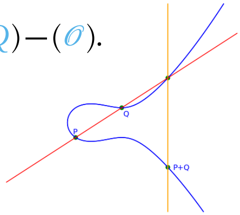
Gives rise to Tate pairing formula:

$$t_m : E(K)[m]\times E(K)/mE(K)\to K^*/(K^*)^m$$

$$t_m(P,Q)=f_P(D_Q),\quad \mathrm{div}(f_P)=m(P)-m(\mathscr{O}),\quad D_Q\sim(Q)-(\mathscr{O}).$$

Tate pairing computation (Miller's Algorithm)

$$t_m(P, Q) = f_P(D_Q), \quad \mathrm{div}(f_P) = m(P) - m(\mathcal{O}), \quad D_Q \sim (Q) - (\mathcal{O}).$$



1. Create double-and-add chain of operations $k_1 + k_2$ for m.
2. This
gives a double-and-add chain of divisors $D_k := k(P) - ([k]P) - (k-1)(\mathcal{O})$
satisfying $D_{k_1} + D_{k_2} \sim D_{k_1+k_2}$. Note that $\mathrm{div}(f_P) = D_m$.
3. Each step
$D_{k_1+k_2} - D_{k_1} - D_{k_2} = ([k_1]P) + ([k_2]P) - ([k_1+k_2]P) - (\mathcal{O})$ is an instance
of the group law, i.e. a rational function f_{k_1,k_2}. Thus $f_P = \prod f_{k_{i,1},k_{i,2}}$.
4. Compute the double-and-add chain to
compute $f_P(D_Q) = \prod f_{k_{i,1},k_{i,2}}(D_Q)$ (always evaluated, i.e. elements of K^*).

Sesquilinear pairings

Let $\alpha, \beta \in \mathcal{O}$, an order in an imaginary quadratic field. A sesquilinear pairing is a bilinear pairing with:

$$\langle \alpha P, \beta Q \rangle = \langle P, Q \rangle^{\alpha \overline{\beta}}.$$

(We can also do everything today with $\mathcal{O}$ a quaternion order, at the cost of lots of extra notation.)

Calculus of $\mathscr{O}$-divisors

Extend scalars:

$$\mathrm{Div}_{\mathscr{O}}(E) := \mathscr{O} \otimes_{\mathbb{Z}} \mathrm{Div}(E).$$

We also extend scalars on $K(E)^*$ and K^*, writing multiplicatively, e.g. g^{1+i}.
Principal divisors:

$$\mathrm{div}\left(\prod_i f_i^{\tau_i}\right) = \sum_i \tau_i \,\mathrm{div}(f_i).$$

Then

$$\mathrm{Pic}^0_{\mathscr{O}}(E) := \mathscr{O} \otimes_{\mathbb{Z}} \mathrm{Pic}^0(E).$$

Evaluating an $\mathcal{O}$-function at an $\mathcal{O}$-divisor

If f and D are usual function and divisor, then

$$f^{\alpha}(\beta \cdot D) := f(D)^{\alpha\overline{\beta}}.$$

This gives $\mathcal{O}$-Weil reciprocity:

$$f(\mathrm{div}(g)) = \overline{g(\mathrm{div}(f))},$$

where conjugation acts on the scalars.

Weil and Tate pairings

Recall: $E \cong \mathrm{Pic}^0(E)$, $\quad P \mapsto (P) - (\mathcal{O})$.

$$e_m : \mathrm{Pic}^0(E)[m] \times \mathrm{Pic}^0(E)[m] \to \mathbb{G}_m[m],$$
$$t_m : \mathrm{Pic}^0(E)[m] \times \mathrm{Pic}^0(E)/[m]\mathrm{Pic}^0(E) \to \mathbb{G}_m/(\mathbb{G}_m)^m,$$

given by

$$t_m(D_P, D_Q) = f_P(D_Q) \quad \text{where} \quad \mathrm{div}(f_P) \sim m \cdot D_P,$$
$$e_m(D_P, D_Q) = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

Galois invariant, sesquilinear, compatible, etc.

Sesquilinear pairings

$$
\begin{aligned}
W_\alpha &: \mathrm{Pic}^0_{\mathcal{O}}(E)[\overline{\alpha}] \times \mathrm{Pic}^0_{\mathcal{O}}(E)[\alpha] \to \mathbb{G}_m^{\otimes_{\mathbb{Z}} \mathcal{O}}[\overline{\alpha}],\\
T_\alpha &: \mathrm{Pic}^0_{\mathcal{O}}(E)[\overline{\alpha}] \times \mathrm{Pic}^0_{\mathcal{O}}(E)/[\alpha]\mathrm{Pic}^0_{\mathcal{O}}(E) \to \mathbb{G}_m^{\otimes_{\mathbb{Z}} \mathcal{O}}/(\mathbb{G}_m^{\otimes_{\mathbb{Z}} \mathcal{O}})^{\overline{\alpha}},
\end{aligned}
$$

given by

$$
T_\alpha(D_P, D_Q) = f_P(D_Q) \quad \text{where} \quad \mathrm{div}(f_P) \sim \overline{\alpha} \cdot D_P,
$$

$$
W_\alpha(D_P, D_Q) = \frac{f_P(D_Q)}{f_Q(D_P)}.
$$

Galois invariant, sesquilinear, compatible, etc.

Moving from formal to CM by $\mathscr{O} = \mathbb{Z}[\tau]$

$$0 \longrightarrow E \xrightarrow{\eta} \mathrm{Pic}^0_{\mathscr{O}}(E) \xrightarrow{\epsilon} E \longrightarrow 0$$

$$\epsilon : \quad D_1 + \tau \cdot D_2 \quad \mapsto \quad D_1^{\Sigma} + [\tau] D_2^{\Sigma}.$$

$$\eta : \quad P \quad \mapsto \quad ([-\tau]P) - (\mathscr{O}) + \tau((P) - (\mathscr{O})).$$

where $\left(\sum \alpha_i (P_i)\right)^{\Sigma} = \sum_i [\alpha_i] P_i$.

A Weil-like pairing

$$\widehat{W}_\alpha : E[\overline{\alpha}] \times E[\alpha] \to \mathbb{G}_m^{\otimes_{\mathbb{Z}} \mathscr{O}}[\alpha].$$

1. Well-defined, bilinear, Galois invariant, **non-degenerate**.
2. Sesquilinearity:
$$\widehat{W}_\alpha([\gamma]P, [\delta]Q) = \widehat{W}_\alpha(P,Q)^{\delta\overline{\gamma}}.$$
3. Conjugate skew-Hermitian:
$$\widehat{W}_\alpha(P,Q) = \overline{\widehat{W}_{\overline{\alpha}}(Q,P)}^{\,-1}.$$
4. Compatibility: Let $\phi : E \to E'$ respect CM by $\mathscr{O}$.
$$\widehat{W}_\alpha(\phi P, \phi Q) = \widehat{W}_\alpha(P,Q)^{\deg \phi}.$$
5. Coherence:
$$\widehat{W}_{\alpha\beta}(P,Q) = \widehat{W}_\alpha([\overline{\beta}]P, Q), \quad \widehat{W}_{\alpha\beta}(P,Q) = \widehat{W}_\beta(P, [\alpha]Q).$$

A Tate-like pairing

$$\widehat{T}_\alpha : E[\overline{\alpha}] \times E/[\alpha]E \to \mathbb{G}_m^{\otimes_{\mathbb{Z}} \mathcal{O}} / (\mathbb{G}_m^{\otimes_{\mathbb{Z}} \mathcal{O}})^\alpha.$$

1. Well-defined, bilinear, Galois invariant, **non-degenerate**.
2. Sesquilinearity:
$$\widehat{T}_\alpha([\gamma]P, [\delta]Q) = \widehat{T}_\alpha(P, Q)^{\overline{\gamma}\delta}.$$
3. Compatibility: Let $\phi : E \to E'$ respect CM by $\mathcal{O}$.
$$\widehat{T}_\alpha(\phi P, \phi Q) = \widehat{T}_\alpha(P, Q)^{\deg \phi}.$$
4. Coherence:
$$\widehat{T}_{\alpha\beta}(P, Q) \bmod (\mathbb{G}_m^{\otimes_{\mathbb{Z}} R})^\alpha = \widehat{T}_\alpha([\overline{\beta}]P, Q \bmod [\alpha]E).$$
$$\widehat{T}_{\alpha\beta}(P, Q) \bmod (\mathbb{G}_m^{\otimes_{\mathbb{Z}} R})^\beta = \widehat{T}_\beta(P, [\alpha]Q \bmod [\beta]E).$$

In terms of usual Weil and Tate pairings

Let $\mathcal{O} = \mathbb{Z}[\tau]$.

$$\widehat{T}_n(P,Q) = \left(t_n(P,Q)^{2N(\tau)} t_n([-\overline{\tau}]P,Q)^{Tr(\tau)}\right)(t_n([\overline{\tau}-\tau]P,Q))^{\tau}.$$

Furthermore, provided both of the following quantities are defined,

$$\widehat{T}_{N(\alpha)}(P,Q) = \widehat{T}_{\alpha}(P,Q)^{\overline{\alpha}} \pmod{(\mathbb{G}_m^{\otimes_{\mathbb{Z}} R})^{\alpha}}$$

Remark: Let $\langle x, y \rangle$ be a bilinear pairing on $\mathbb{Z}[\tau]$. Then

$$\langle x_1 + \tau x_2, y_1 + \tau y_2 \rangle := \langle x_1, y_1 \rangle + N(\tau)\langle x_2, y_2 \rangle + Tr(\tau)\langle x_1, y_2 \rangle + \tau(\langle x_2, y_1 \rangle - \langle x_1, y_2 \rangle)$$

defines a sesquilinear pairing.

Generalized pairings: Bruin, Garefalakis, Robert, Castryck-Houben-Merz-Mula-van Buuren-Vercauteren

Computation of $\widehat{T}_{\alpha}(P, Q)$

Suppose

$$\overline{\alpha} = d - c\tau, \quad \overline{\alpha}\tau = -b + a\tau.$$

For $P \in E[\overline{\alpha}]$, $f_P = f_{P,1} f_{P,2}^{\tau}$ with

$$\operatorname{div}(f_{P,1}) = a([-\tau]P) + b(P) - (a+b)(\mathcal{O}), \quad \operatorname{div}(f_{P,2}) = c([-\tau]P) + d(P) - (c+d)(\mathcal{O}).$$

Auxiliary point S; take $D_Q = D_{Q,1} + \tau \cdot D_{Q,2}$ with

$$D_{Q,1} = ([-\tau]Q + [-\tau]S) - ([-\tau]S), \quad D_{Q,2} = (Q+S) - (S).$$

Then

$$\widehat{T}_{\alpha}(P, Q) := f_P(D_Q) =$$

$$\left(f_{P,1}(D_{Q,1}) f_{P,1}(D_{Q,2})^{Tr(\tau)} f_{P,2}(D_{Q,2})^{N(\tau)}\right)\left(f_{P,2}(D_{Q,1}) f_{P,1}(D_{Q,2})^{-1}\right)^{\tau}.$$

Applications to Isogenies (joint with Joseph Macula)

Finite $\mathbb{F}$. There is a faithful action of $\mathrm{Cl}(\mathcal{O})$ on

$$\mathrm{Ell}(\mathcal{O}) = \{E/\mathbb{F} : E \text{ has CM by } \mathcal{O}\}.$$

When $\mathfrak{a} \cdot E_1 = E_2$, this gives an isogeny $\phi_{\mathfrak{a}} : E_1 \to E_2$ respecting $\mathcal{O}$.

Hard Problem 1: Given E_1 and $E_2 \in \mathrm{Ell}(\mathcal{O})$, find $\phi : E_1 \to E_2$ respecting $\mathcal{O}$.

Hard Problem 2: Given E_1 and $E_2 \in \mathrm{Ell}(\mathcal{O})$, and $\deg \phi$, find $\phi : E_1 \to E_2$ respecting $\mathcal{O}$.

Isogeny interpolation
(Castryck-Decru-Maino-Martindale-Panny-Pope-Robert-Wesolowski)

Hard Problem 2: Given E_1 and $E_2 \in \mathrm{Ell}(\mathcal{O})$, and $\deg \phi$, find $\phi : E_1 \to E_2$ respecting $\mathcal{O}$.

Wouter's talk [CDM+24]: to efficiently determine $\phi : E_1 \to E_2$, it suffices to find $\phi(G)$ (actually ϕ of generators) for some subgroup G of size at least $4 \deg \phi + 1$.

Hard Problem 3: Given E_1 and $E_2 \in \mathrm{Ell}(\mathcal{O})$, and $\deg \phi$, find $\phi(G)$, $\#G > 4 \deg \phi$ for $\phi : E_1 \to E_2$ respecting $\mathcal{O}$.

Recovering an isogeny

An idea of Castryck-Houben-Merz-Mula-van Buuren-Vercauteren: Let $m > 4\deg\phi$.
Suppose $P \in E_1[m]$, and suppose $\phi(P) = kP' \subseteq E_2[m]$. Use a pairing:

$$\langle P, P\rangle^{\deg\phi} = \langle \phi P, \phi P\rangle = \langle kP', kP'\rangle = \langle P', P'\rangle^{k^2}.$$

So

$$P, P', \deg\phi \xrightarrow{\text{discrete log}} k^2 \pmod m \implies \phi P = kP' \xrightarrow{\text{isog. interp.}} \phi.$$

Challenges:

1. Make sure $\phi P \in \mathbb{Z}P'$.
2. Make sure $\langle P, P\rangle$ is non-trivial.

CHMMvBV: Non-degenerate self-pairings when $m \mid \Delta_{\mathcal{O}}$.

$\mathcal{O}$-sesquilinear pairings

Let $m^2 > 4\deg\phi$. Suppose $P \in E_1[m]$, suppose $\mathcal{O}P' = E_2[m]$. Use a pairing:

$$\langle P, P\rangle^{\deg\phi} = \langle \phi P, \phi P\rangle = \langle \lambda P', \lambda P'\rangle = \langle P', P'\rangle^{N(\lambda)}.$$

So

$$P, P', \deg\phi \quad \xRightarrow{\text{discrete log}} \quad N(\lambda) \pmod m \quad \not\Rightarrow \quad \phi P = [\lambda]P' \quad \xRightarrow{\text{isog. interp.}} \quad \phi.$$

Pros/Cons:

1. Easier to guarantee $\mathcal{O}P' = E_2[m]$.
2. Easier to obtain non-degenerate pairings (m coprime to $\Delta_{\mathcal{O}}$).
3. For m coprimes to $\Delta_{\mathcal{O}}$, knowing $N(\lambda) \pmod m$ only cuts down $\lambda \pmod m$ from $\sim m^2$ options to $\sim m$ options.
4. For $m \mid \Delta_{\mathcal{O}}$ it works! And is sometimes more efficient.

When is $\widehat{T}_m$ non-degenerate?

Let $\eta : \mathcal{O} \to \mathrm{End}(E)$ extend to $\eta : K \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$.

Proposition (Macula-S.)

$E[m]$ is $\mathcal{O}$-cyclic as an $\mathcal{O}$-module if and only if m is coprime to $[\eta(K) \cap \mathrm{End}(E) : \eta(\mathcal{O})]$.

Based on results of Lenstra.

Theorem (Macula-S.)

Suppose $\mu_m \subseteq \mathbb{F}$, m is coprime to $\Delta_{\mathcal{O}}$, and $E[m] \subseteq E(\mathbb{F})$. Then $\widehat{T}_n(P,P)$ has full order whenever $\mathcal{O}P = E[m]$.

Computation of $\mathcal{O}$-pairings

Theorem (Macula-S.)

Suppose computations in $\mathbb{F}$ *and* $E[m]$*, and discrete logarithms in* μ_m *are all efficient.*
Let m *be coprime to* $\Delta_{\mathcal{O}}$ *and let* $\mathcal{O} \subseteq \mathrm{End}(E)$.
Then

$$\textit{computation of the } \mathcal{O}\textit{-pairing } \widehat{T}_m(P,Q) \textit{ on } E[m]$$

$$\textit{is equivalent to}$$

$$\textit{computation of } \mathcal{O} \textit{ acting on } E[m].$$

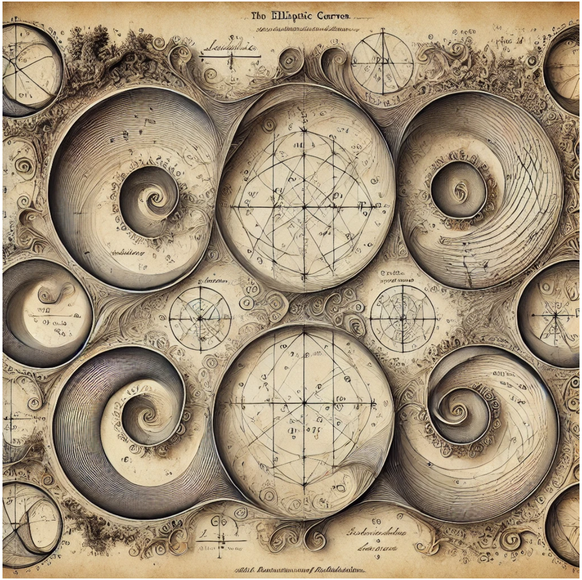
A trade-off (Supersingular case)

Suppose $m^2 > 4 \deg \phi$, coprime to $\Delta_{\mathscr{O}}$ and $\deg \phi$.

Situations where we can obtain ϕ:

Know full $\phi(E_1[m])$	Known $\phi(\langle P \rangle)$, $P \in E_1[m]$ and $\mathscr{O} \subseteq \mathrm{End}(E_i)$ (S.-Macula)	Know full $\mathrm{End}(E_i)$

Thank you!



Temporary page!

LaTeX was unable to guess the total number of pages correctly. As there was some unprocessed data that should have been added to the final page this extra page has been added to receive it.

If you rerun the document (without altering it) this surplus page will go away, because LaTeX now knows how many pages to expect for this document.