# *The Weil Pairing*

*Scribe: Matthew Stevens*

*March 9, 2022*

The following is a WIP typed adaptation of Dr. Andreas Mihatsch's notes on the Weil pairing, available here: https://www.math.uni-bonn.de/people/mihatsch/21u22%20WS/moduli/.

## The Pairing

Let $E$ be an elliptic curve over $S$.

Recall that the contravariant functor

$$\mathrm{Pic}^0_{E/S} : \mathbf{Sch}/S \to \mathbf{Set} : T \mapsto \mathrm{Pic}^0(T \times_S E)/p_T^* \mathrm{Pic}(T)$$

is representable. Its universal object $\widehat{E}/S$ is called the **dual elliptic curve**. It is isomorphic to $E$ as an $S$-scheme via the map $p \mapsto \mathcal{O}_E([p] - [e])$.

Let $\mu_{n,S}$ denote the group scheme of roots of unity of $S$.

See Stacks [040M] for more information about $\mu_{n,S}$.

Our aim is to construct a bilinear pairing $e_n : E[n] \times \widehat{E}[n] \to \mu_{n,S}$. We will sometimes regard $e_n$ as a pairing $E[n] \times E[n] \to \mu_{n,S}$ via the canonical isomorphism $E \to \widehat{E}$.

First, suppose that $S$ is equal to the spectrum of an algebraically closed field $k$. Let $x$ be a point in $E[n](k)$ and let $L$ be an element of $\widehat{E}[n]$, i.e. let $L$ be a degree 0 line bundle on $E$ such that $L^{\otimes n}$ is isomorphic to $\mathcal{O}_E$. Write $L \cong \mathcal{O}([y] - [e])$.

Fix $y' \in E(k)$ such that $ny'$ equals $y$. Then, we have $[n^2]y' = 0$. Since $E[n](k)$ consists of $n^2$ elements, the sum $\sum_{x \in E[n](k)} (x' + y' - x')$ equals 0. Thus, there exists a meromorphic function $f$ on $E$ such that we have

The fact that $E$ is isomorphic as a group scheme to $\mathrm{Pic}^0_{E/S}$ means that a divisor on $E$ is principle if and only if the corresponding sum in $E$ is trivial! We'll use this crucial observation repeatedly.

$$\mathrm{div}(f) = [n]^{-1}([y] - [e]) = \sum_{x' \in E[n](k)} [x' + y'] - [x'].$$

One readily verifies that $t_x^*(f)$ has the same divisor as $f$, so $t_x^*(f)$ and $f$ differ by a constant. Now, we define $e_n(x, L)$ to be $(t_x^* f)/f \in k^\times$. When regarding $e_n$ as a pairing with domain $E[n] \times E[n]$ rather than $E[n] \times \widehat{E}[n]$, we will write $e_n(x, y)$ instead of $e_n(x, L)$.

"Translation on top". The notes have $t_x^* f$ in the denominator, but I think that was a typo.

Now, for a general base scheme $S$, let $x$ be an element of $E[n](S)$. Let $L$ be an element of $\widehat{E}[n](S)$. After restricting to a sufficiently small open $U$ in $S$, we can pick a trivialization $\psi : \mathcal{O}_E \xrightarrow{\sim} [n]^* L$, which is unique up to an element of $\mathcal{O}_S^\times$. Since $t_x$ is an isomorphism, we get an isomorphism $\mathcal{O}_E \xrightarrow{\sim} t_x^* \mathcal{O}_E$. Composing with the map $t_x^* \psi : t_x^* \mathcal{O}_E \xrightarrow{\sim} t_x^*([n]^* L)$, we get a map $\psi_x : \mathcal{O}_E \cong t_x^*([n]^* L)$. Now, we have $t_x^*([n]^* L) = ([n] \circ t_x)^* L = [n]^* L$, where the last step follows from the fact that $x$ is an $n$-torsion point; in particular, the map $\psi_x$ is an isomorphism $\mathcal{O}_E \xrightarrow{\sim} [n]^* L$. Thus, there exists a unit $u$ over $U$ such that $\psi_x$ equals $u\psi$.

For $T$-valued points, this same discussion goes through after base-changing by $T$.

**Definition-Theorem 1.** *1. The constant $u$ over $U \subseteq S$ arising from our choice of $\psi$ in the previous paragraph is independent of the choice of $\psi$. Thus, by repeating the*

*above construction for the various $U \subseteq S$ on which $[n]^*L$ is trivial and gluing, we get a global section $s \in \mathcal{O}_S^\times(S)$. In particular, the process described in the previous paragraph yields a function $e_n(x, L) \colon E[n] \times \widehat{E}[n] \to \mathcal{O}_S^\times(S)$.*

2. *The function $e_n$ is bilinear and takes values in $\mu_{n,S} = \{\xi \in \mathcal{O}_S^\times(S) : \xi^n = 1\}$. We call $e_n$ the **Weil pairing** with respect to the n-torsion of E. As before, if L is the line bundle corresponding to a point $y \in E[n]$, we sometimes write $e_n(x, y)$ in place of $e_n(x, L)$.*

3. *The Weil pairing is alternating, i.e., for any $y \in E[n]$, we have $e_n(y, y) = 1$.*

4. *For every $y_1 \in E[nm]$ and every $y_2 \in E[n]$, we have $e_{nm}(y_1, y_2) = e_n(my_1, y_2)$.*

*Proof.* To see that (1) holds, suppose that $\lambda\psi \colon \mathcal{O}_E \xrightarrow{\sim} [n]^*L$ is another choice of trivialization for $[n]^*L$ on $U \subseteq S$. We have $t_x^*(\lambda\psi) = \lambda t_x^*(\psi) = u\lambda\psi = u(\lambda\psi)$. Thus, the constant $u$ is independent of our choice of trivialization and we get a well-defined map $E[n] \times \widehat{E}[n] \to \mathcal{O}_S(S)$.

Now, let's prove (2), (3), and (4). We claim that it suffices to assume that $S$ is an algebraically closed field of characteristic 0. To see this, first note that by the local nature of the statements in question, it suffices to work at each $\mathcal{O}_{S,s}$ for each $s \in S$, so we can assume that $S$ is the spectrum of a local ring and, in particular, that $\omega_E$ is trivial. The triviality of $\omega_E$ implies that we can put $E$ into Weierstrass form $Y^2 + c_1XY + c_3Y = X^3 + c_2X^2 + c_4X + c_6$. Now, over the base $\operatorname{Spec} \boldsymbol{Z}[a_1, \dots, a_6][\Delta^{-1}]$, we have the elliptic curve $\mathscr{E}$ cut out by $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$. The elliptic curve $E/S$ arises as a pullback of $\mathscr{E}/\operatorname{Spec} \boldsymbol{Z}[a_1, \dots, a_6][\Delta^{-1}]$. One readily verifies that if (2), (3), and (4) are preserved by base-change, so it suffices to prove them for $\mathscr{E}/\operatorname{Spec} \boldsymbol{Z}[a_1, \dots, a_6][\Delta^{-1}]$. Since $\operatorname{Spec} \boldsymbol{Z}[a_1, \dots, a_6][\Delta^{-1}]$ arises from inverting an element in a polynomial ring in finitely many variables over $\boldsymbol{Z}$, and $\boldsymbol{C}$ has infinite transcendence degree over $\boldsymbol{Q}$, it suffices to treat the case in which $E$ is an elliptic curve over $\boldsymbol{C}$.

Under this assumption, let's prove (2), (3), and (4). Suppose that $x_1, x_2$, and $y_2$ are elements of $E[n]$. We have

$$\begin{aligned} e_n(x_1 + x_2, y) &= \frac{t_{x_1+x_2}(f)}{f} \\ &= \frac{t_{x+1+x_2}^*}{t_{x_1}^*(f)} \cdot \frac{t_{x_1}^*(f)}{f} \\ &= t_{x_1}^* \left( \frac{t_{x_2}^*(f)}{f} \right) \frac{t_{x_1}^*(f)}{f} \\ &= t_{x_1}^*(e_n(x_1, y)) \cdot e_n(x_2, y) \\ &= e_n(x_1, y) e_n(x_2, y), \end{aligned}$$

This step follows because constants are translation invariant!

which proves that $e_n$ is linear in the first argument. Linearity in the second argument is clear from the definition.

Linearity in the first argument implies that $e_n(x, y)^n$ equals $e(nx, y)$. Since $x$ lies in $E[n]$, we have $nx = 0$, so $e(nx, y)$ equals $e(0, y)$. Linearity in the first argument implies that $e(0, y)$ equals 1, so $e_n$ takes values in $\mu_{n,S}$ and (2) is proved.

Now, let's prove (3). Let $y$ be an element of $E[n]$. Since $\mathcal{O}([y] - [e])$ is $n$-torsion in $\widehat{E}$, there exists a meromorphic function $g$ on $E$ such that $\operatorname{div}(g)$ equals $n[y] - n[e]$. Consider the function $\prod_{i=0}^{n-1} t_{iy}^* g$. The divisor $\operatorname{div}(\prod_{i=0}^{n-1} t_{iy}^* g)$ is the sum $n \sum_{i=0}^{n-1} [(i-i)y] - [-iy]$ which telescopes and simplifies to 0. Thus, the function $\prod_{i=0}^{n-1} t_{iy}^* g$ is constant. Let $f$ be a meromorphic function such that $\operatorname{div}(f)$ equals $[n]^{-1}([y]-[e])$. The functions $f^n$ and $g \circ [n]$ differ by multiplication by a constant. Let $y'$ be such that $ny'$ equals $y$. Then, we have that $(\prod_{i=0}^{n-1} t_{iy'}^* f)^n$ differs from $(\prod_{i=0}^{n-1} t_{iy}^* g) \circ [n]$ by multiplication by a constant. Since $\prod_{i=0}^{n-1} t_{iy}^* g$ is constant, so is $\prod_{i=0}^{n-1} t_{iy'}^* f$. To say that $\prod_{i=0}^{n-1} t_{iy'}^* f$ is constant is to say that it is translation-invariant, so for every point $z$, we have $\prod_{i=0}^{n-1} f(z + iy') = \prod_{i=0}^{n-1} f(z + (i+1)y')$. This implies that for every $z$ such that $\prod_{i=0}^{n-1} f(z + iy')$ is nonzero, we have $f(z) = f(z + ny') = f(z + y)$; since $f$ and $t_y^*(f)$ differ by multiplication by a constant (or, alternatively, since $f$ has only a single zero), the functions $t_y^*(f)$ and $f$ must coincide identically. In particular, we have $e_n(y, y) = 1$. This proves (3).

Remember, the fact that $t_y^*(f)$ and $f$ differ by a constant was used to show that $e_n$ is well-defined; to show that $e_n(y, y)$ is 1, we technically only need to show that $f$ and $t_y^*(f)$ coincide for even a single input.

Let $y_1$ be an element of $E[nm]$ and let $y_2$ be an element of $E[n]$. Let $f$ be a function such that $\operatorname{div}(f)$ equals $[n]^{-1}([y_2] - [e])$. Then, the divisor $\operatorname{div}(f \circ [m])$ equals $[nm]^{-1}([y] - [e])$. Thus, we have

$$\begin{aligned} e_{nm}(y_1, y_2) &= \frac{t_{y_1}^*(f \circ [m])}{f \circ [m]} \\ &= \left(\frac{f}{t_{mx}^*(f)}\right) \circ [m] \\ &= \left(\frac{f}{t_{mx}^*(f)}\right) \\ &= e_n(mx, y), \end{aligned}$$

which proves (4). □

**Lemma 2.** *Let $x$ and $y$ be elements of $E[n]$. We have $e_n(x, y) = e_n(y, x)^{-1}$.*

*Proof.* Since $e_n$ is alternating, we have $e_n(x + y, x + y) = 1$. By bilinearity, we have $e_n(x + y, x + y) = e(x, x)e(x, y)e(y, x)e(y, y)$. Since $e_n$ is alternating, both $e(x, x)$ and $e(y, y)$ are equal to 1, so we have $e(x, y)e(y, x) = 1$. □

**Lemma 3.** *If $S$ is the spectrum of an algebraically closed field $k$ such that* char *$k$ does not divide $n$, then the Weil pairing is nondegenerate.*

*Proof.* Suppose that $y$ is an element of $E[n]$ is an element such that for all $x \in E[n]$, there holds $e_n(x, y) = 1$. This means that if $f$ is a meromorphic function on $E$ with $\operatorname{div}(f) = n^{-1}([y] - [e])$, then $f$ is invariant under translation by elements of $E[n]$. Now, let $h$ be such that $f$ equals $h \circ [n]$ and let $g$ be a function such that $\operatorname{div}(g)$ equals $n[y] - n[e]$. Then, the functions $f^n$ and $g \circ [n]$ differ by multiplication by a constant. Thus, the functions $(h \circ [n])^n$ and $g \circ [n]$ differ by multiplication by a constant. This implies that $g$ and $h^m$ differ by multiplication by a constant. Thus, we have $\operatorname{div}(h) = [y] - [e]$. Thus, the points $y$ and $e$ coincide. □