Math 7359 (Elliptic Curves and Modular Forms)

Lecture #17 of 24 $\sim$ November 6, 2023

The Weil Pairing and the Weil Conjectures (Again)

- The Weil Pairing
- Properties of the Weil Pairing
- Proof of the Weil Conjectures for Elliptic Curves

Recall

Recall the Tate module:

Definition

Let E be an elliptic curve and l be a prime. The l-adic Tate module of E is the $\mathbb{Z}_l$-module $T_l(E) = \varprojlim_d E[l^d]$.

The elements of the Tate module consist of sequences of points $(P_1, P_2, P_3, P_4, \dots)$ such that $lP_{d+1} = P_d$ for each $d \geq 0$, where we think of $P_0 = O$.

Recall

Recall the Tate module:

Definition

Let E be an elliptic curve and l be a prime. The l-adic Tate module of E is the $\mathbb{Z}_l$-module $T_l(E) = \varprojlim_d E[l^d]$.

The elements of the Tate module consist of sequences of points $(P_1, P_2, P_3, P_4, \dots)$ such that $lP_{d+1} = P_d$ for each $d \geq 0$, where we think of $P_0 = O$.

- When $l \neq \mathrm{char}(k)$, when we apply the inverse limit construction starting with generators P and Q of $E[l]$, we obtain topological generators for $T_l(E)$ yielding a group isomorphism $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$.

Motivation for the Weil Pairing, I

The remaining ingredient for our plan in proving the Weil conjectures is to find an analogue of an inner product structure associated to the action of the Galois group on $\mathrm{Aut}[T_l(E)]$.

- As with our construction of the Tate module, we will do this by constructing a pairing on the components $E[l^d]$ used in the inverse limit construction of $T_l(E)$.
- Indeed, for no additional cost, we can construct the pairing on $E[m]$.

Motivation for the Weil Pairing, I

The remaining ingredient for our plan in proving the Weil conjectures is to find an analogue of an inner product structure associated to the action of the Galois group on $\mathrm{Aut}[T_l(E)]$.

- As with our construction of the Tate module, we will do this by constructing a pairing on the components $E[l^d]$ used in the inverse limit construction of $T_l(E)$.
- Indeed, for no additional cost, we can construct the pairing on $E[m]$.
- Fix a positive integer $m \geq 2$ not divisible by $p = \mathrm{char}(k)$.
- Since we are being informal and lazy for now, we may as well choose a basis $\{P, Q\}$ of $E[m]$, yielding an isomorphism $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.
- Then elements are of the form $aP + bQ$ for $a, b \in \mathbb{Z}/m\mathbb{Z}$.

Motivation for the Weil Pairing, II

A natural pairing with many convenient properties is

$$\langle aP + bQ, cP + dQ\rangle = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \pmod{m}.$$

- For instance, the pairing is bilinear, alternating, and nondegenerate, all of which are properties we would want for something analogous to an inner product.

Motivation for the Weil Pairing, II

A natural pairing with many convenient properties is

$$\langle aP + bQ, cP + dQ \rangle = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \pmod{m}.$$

- For instance, the pairing is bilinear, alternating, and nondegenerate, all of which are properties we would want for something analogous to an inner product.
- Of course this pairing does not take values in a field unless m is prime, but we can easily deal with this shortcoming by instead using $\langle aP + bQ, cP + dQ \rangle = \zeta^{ad-bc}$ where $\zeta \in k$ is some primitive mth root of unity.
- However, this construction relies on several choices (the basis $\{P, Q\}$ and the mth root of unity ζ). In order to take an inverse limit, we want to give a more natural pairing that doesn't depend on particular choices of basis and generator for the group of mth roots of unity.

Motivation for the Weil Pairing, III

So let's try to do something more canonical.

- First, for any $Q \in E[m]$, since the divisor $m[Q] - m[O]$ has degree 0 and the sum of points resolves to the identity on E, it is principal: say $m[Q] - m[O] = \mathrm{div}(f_Q)$, for a function $f_Q \in k(C)$ unique up to scaling.
- We claim that the divisor $[m]^* Q - [m]^* O$ is also principal.

Motivation for the Weil Pairing, III

So let's try to do something more canonical.

- First, for any $Q \in E[m]$, since the divisor $m[Q] - m[O]$ has degree 0 and the sum of points resolves to the identity on E, it is principal: say $m[Q] - m[O] = \mathrm{div}(f_Q)$, for a function $f_Q \in k(C)$ unique up to scaling.
- We claim that the divisor $[m]^*Q - [m]^*O$ is also principal.
- To see this choose any $Q' \in [m]^{-1}Q$: then by definition we have $[m]^*Q - [m]^*O = \sum_{R \in E[m]}([Q' + R] - [R])$ which is also principal since it has degree 0 and the underlying sum of points is $\sum_{R \in E[m]} Q' = [m^2]Q' = [m]Q = O$.
- This means $[m]^*Q - [m]^*O = \mathrm{div}(g_Q)$ for some function g_Q that is unique up to scaling.

Motivation for the Weil Pairing, IV

We have $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$.

Motivation for the Weil Pairing, IV

We have $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$.

- Then $\mathrm{div}(g_Q^m) = \sum_{R \in E[m]}(m[Q' + R] - m[R])$ and also $\mathrm{div}(f_Q \circ [m]) = \sum_{R \in E[m]}(m[Q' + R] - m[R])$.
- Thus g_Q^m and $f_Q \circ [m]$ have the same divisor, meaning that they differ by a nonzero scalar factor (since the divisor of their ratio is zero, hence is constant).
- Hence by rescaling f_Q, we may assume that $f_Q \circ [m] = g_Q^m$.

Motivation for the Weil Pairing, IV

We have $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$.

- Then $\mathrm{div}(g_Q^m) = \sum_{R \in E[m]}(m[Q' + R] - m[R])$ and also $\mathrm{div}(f_Q \circ [m]) = \sum_{R \in E[m]}(m[Q' + R] - m[R])$.
- Thus g_Q^m and $f_Q \circ [m]$ have the same divisor, meaning that they differ by a nonzero scalar factor (since the divisor of their ratio is zero, hence is constant).
- Hence by rescaling f_Q, we may assume that $f_Q \circ [m] = g_Q^m$.
- Now suppose we have some other point $P \in E[m]$.
- Then for any $X \in E$, we see that $g_Q(X + P)^m = f_Q([m]X + [m]P) = f_Q([m]X) = g_Q(X)^m$.
- Thus, as long as $g_Q(X)$ is not zero or ∞, the ratio $g_Q(X + P)/g_Q(X)$ is some mth root of unity.

Motivation for the Weil Pairing, V

Exercise: Suppose $h \in k(E)$ is a rational function that takes only finitely many values on E. Show that h is constant. (Note as always that k is algebraically closed.)

- By the exercise, since $g_Q(X+Q)/g_Q(X) \in k(E)$ takes only finitely many values, it must in fact be constant, so it is independent of X.
- Furthermore, since g is defined uniquely up to a constant factor, the ratio $g_Q(X+P)/g_Q(X)$ is independent of the specific choice of g.
- Thus, we obtain a well-defined pairing $e_m(P,Q) = g_Q(X+P)/g_Q(X)$ from $E[m] \times E[m]$ to the multiplicative group of mth roots of unity $\mu_m = \{\zeta \in k : \zeta^m = 1\}$ in k.

The Weil Pairing, I

This pairing is called the Weil pairing:

Definition

Let E/k be an elliptic curve and $m \geq 2$ be an integer not divisible by $p = \mathrm{char}(k)$.

The Weil pairing $e_m : E[m] \times E[m] \to \mu_m$ is defined as follows: for any $P, Q \in E[m]$, choose any $g_Q \in k(C)$ such that $\mathrm{div}(g_Q) = [m]^* Q - [m]^* O$, and then define $e_m(P, Q) = g_Q(X + P)/g_Q(X)$ for any $X \in E$ such that the ratio is defined.

From our discussion above, the definition of $e_m(P, Q)$ is independent from the specific choice of the function g_P and from the choice of the point X where the ratio is evaluated.

The Weil Pairing, II

And now, briskly into the properties:

Proposition (Properties of the Weil Pairing)

Let E be an elliptic curve and $m \geq 2$ be an integer not divisible by $p = \mathrm{char}(k)$, with $e_m : E[m] \times E[m] \to \mu_m$ the Weil pairing on E. Then the following hold:

1. *(Bilinearity) We have $e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$ and $e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$.*
2. *(Alternating) We have $e_m(P, P) = 1$ for all $P \in E[m]$, or equivalently, $e_m(P, Q) = e_m(Q, P)^{-1}$ for all $P, Q \in E[m]$.*
3. *(Nondegeneracy) If $e_m(P, Q) = 1$ for all $P \in E[m]$ then $Q = O$.*
4. *(Galois-equivariance) If E is defined over F, then for any $\sigma \in \mathrm{Gal}(k/F)$ we have $e_m(\sigma P, \sigma Q) = \sigma[e_m(P, Q)]$.*

The Weil Pairing, III

And now, briskly into the properties:

Proposition (Properties of the Weil Pairing, continued)

Let E be an elliptic curve and $m \geq 2$ be an integer not divisible by $p = \mathrm{char}(k)$, with $e_m : E[m] \times E[m] \to \mu_m$ the Weil pairing on E. Then the following hold:

5. *(Compatibility) For any $P \in E[mm']$ and $Q \in E[m]$ we have $e_{mm'}(P, Q) = e_m([m']P, Q)$.*
6. *(Surjectivity) For any mth root of unity ζ_m, there exist $P, Q \in E[m]$ with $e_m(P, Q) = \zeta_m$.*
7. *(Adjoints) For any isogeny $\varphi : E_1 \to E_2$ and any $P \in E_1[m]$ and $Q \in E_2[m]$, we have $e_m^{(1)}(P, \hat{\varphi}(Q)) = e_m^{(2)}(\varphi(P), Q)$ where $e_m^{(i)}$ is the Weil pairing on E_i.*

The Weil Pairing, IV

1. (Bilinearity 1) We have $e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$.

Proof:

The Weil Pairing, IV

1. (Bilinearity 1) We have $e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$.

Proof:

- We have $e_m(P_1 + P_2, Q) = \dfrac{g_Q(X + P_1 + P_2)}{g_Q(X)} = \dfrac{g_Q(X + P_1 + P_2)}{g_Q(X + P_2)} \cdot \dfrac{g_Q(X + P_2)}{g_Q(X)} = e_m(P_1, Q)e_m(P_2, Q)$ since $\dfrac{g_Q(X + P_1 + P_2)}{g_Q(X + P_2)} = \dfrac{g_Q(Y + P_1)}{g_Q(Y)}$ for $Y = X + P_2$.

The Weil Pairing, IV: Wasn't the Last One IV?

1. (Bilinearity 2) $e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$.

Proof:

The Weil Pairing, IV: Wasn't the Last One IV?

1. (Bilinearity 2) $e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$.

Proof:

- Let $Q_3 = Q_1 + Q_2$ and take f_i, g_i with $\mathrm{div}(f_i) = m[Q_i] - m[O]$ and $\mathrm{div}(g_i) = [m]^*Q_i - [m]^*O$ so that $f_i \circ [m] = g_i^m$ for each i.
- Since the divisor $[Q_3] - [Q_2] - [Q_1] + [O]$ has degree 0 and resolves to the identity, it is $\mathrm{div}(h)$ for some h.

The Weil Pairing, IV: Wasn't the Last One IV?

1. (Bilinearity 2) $e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$.

Proof:

- Let $Q_3 = Q_1 + Q_2$ and take f_i, g_i with $\operatorname{div}(f_i) = m[Q_i] - m[O]$ and $\operatorname{div}(g_i) = [m]^* Q_i - [m]^* O$ so that $f_i \circ [m] = g_i^m$ for each i.
- Since the divisor $[Q_3] - [Q_2] - [Q_1] + [O]$ has degree 0 and resolves to the identity, it is $\operatorname{div}(h)$ for some h.
- Then $\operatorname{div}(f_3) - \operatorname{div}(f_1 f_2) = m \operatorname{div}(h)$, so $f_3 = cf_1 f_2 h^m$ for some scalar c. Composing with $[m]$ gives $g_3^m = f_3 \circ [m]$ $= (cf_1 f_2 h^m) \circ [m] = c(f_1 \circ [m])(f_2 \circ [m])(h \circ [m])^m =$ $cg_1^m g_2^m (h \circ [m])^m$ so $g_3 = c' g_1 g_2 (h \circ [m])$ for some c'.
- Now we have $e_m(P, Q_1 + Q_2) = \frac{g_3(X+P)}{g_3(X)} = \frac{c' g_1(X+P) g_2(X+P) h([m]X+[m]P)}{c' g_1(X) g_2(X) h([m]X)} =$ $\frac{g_1(X+P)}{g_1(X)} \frac{g_2(X+P)}{g_2(X)} = e_m(P, Q_1)e_m(P, Q_2)$, where $h([m]X + [m]P) = h([m]X)$ since $P \in E[m]$.

The Weil Pairing, IV: No, We're Not Doing This Again

2. (Alternating) We have $e_m(P, P) = 1$ for all $P \in E[m]$, or equivalently, $e_m(P, Q) = e_m(Q, P)^{-1}$ for all $P, Q \in E[m]$.

Proof:

- Take f, g with $\mathrm{div}(f) = m[P] - m[O]$ and $\mathrm{div}(g) = [m]^*P - [m]^*O$ with $g^m = f \circ [m]$.

The Weil Pairing, IV: No, We're Not Doing This Again

2. (Alternating) We have $e_m(P, P) = 1$ for all $P \in E[m]$, or equivalently, $e_m(P, Q) = e_m(Q, P)^{-1}$ for all $P, Q \in E[m]$.

Proof:

- Take f, g with $\mathrm{div}(f) = m[P] - m[O]$ and $\mathrm{div}(g) = [m]^*P - [m]^*O$ with $g^m = f \circ [m]$.
- Now for each k, let $\tau_{-kP} : E \to E$ be the translation map $\tau_{-kP}(X) = X - kP$ and also take $f_k = f \circ \tau_{-kP}$.
- Then $\mathrm{div}(f \circ \tau_{-kP}) = m[(1+k)P] - m[kP]$ since composing with τ_{-kP} simply translates zeroes and poles by kP.
- Then $\mathrm{div}(f_0 f_1 \cdots f_{m-1}) = 0$ since the divisor sum telescopes, meaning that the product $f_0 f_1 \cdots f_{m-1}$ is constant.
- Then for $g_k = g \circ \tau_{-kP'}$ for any P' with $[m]P' = P$, we see that $(g_0 g_1 \cdots g_{m-1})^m = (f_0 f_1 \cdots f_{m-1}) \circ [m]$ is constant whence $g_0 g_1 \cdots g_{m-1}$ is constant.

The Weil Pairing, VI: Wait, Where's V?

2. (Alternating) We have $e_m(P, P) = 1$ for all $P \in E[m]$, or equivalently, $e_m(P, Q) = e_m(Q, P)^{-1}$ for all $P, Q \in E[m]$.

<u>Proof</u> (continued):

- Then for $g_k = g \circ \tau_{-kP'}$ for any P' with $[m]P' = P$, we see that $(g_0 g_1 \cdots g_{m-1})^m = (f_0 f_1 \cdots f_{m-1}) \circ [m]$ is constant whence $g_0 g_1 \cdots g_{m-1}$ is constant.

The Weil Pairing, VI: Wait, Where's V?

2. (Alternating) We have $e_m(P, P) = 1$ for all $P \in E[m]$, or equivalently, $e_m(P, Q) = e_m(Q, P)^{-1}$ for all $P, Q \in E[m]$.

Proof (continued):

- Then for $g_k = g \circ \tau_{-kP'}$ for any P' with $[m]P' = P$, we see that $(g_0 g_1 \cdots g_{m-1})^m = (f_0 f_1 \cdots f_{m-1}) \circ [m]$ is constant whence $g_0 g_1 \cdots g_{m-1}$ is constant. This means
  $g(X)g(X + P') \cdots g(X + (m-1)P')$
  $= g_0(X)g_1(X) \cdots g_{m-1}(X)$
  $= g_0(X + P')g_1(X + P') \cdots g_{m-1}(X + P')$
  $= g(X + P')g(X + 2P') \cdots g(X + mP')$
  and so cancelling the common terms yields
  $g(X) = g(X + mP') = g(X + P)$, whence $e_m(P, P) = 1$.
- For the second statement we have $1 = e_m(P + Q, P + Q) = e_m(P, P)e_m(P, Q)e_m(Q, P)e_m(Q, Q) = e_m(P, Q)e_m(Q, P)$ using bilinearity.

The Weil Pairing, V: Oh, Okay

3. (Nondegeneracy) If $e_m(P, Q) = 1$ for all $P \in E[m]$ then $Q = O$.

Proof:

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$ with $g_Q^m = f_Q \circ [m]$.
- Suppose $e_m(P, Q) = 1$ for all $P \in E[m]$, meaning that $g_Q(X + P) = g_Q(X)$ for all $P \in E[m]$.

The Weil Pairing, V: Oh, Okay

3. (Nondegeneracy) If $e_m(P,Q)=1$ for all $P \in E[m]$ then $Q=O$.

Proof:

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$ with $g_Q^m = f_Q \circ [m]$.
- Suppose $e_m(P,Q) = 1$ for all $P \in E[m]$, meaning that $g_Q(X+P) = g_Q(X)$ for all $P \in E[m]$.
- This means $g_Q \circ \tau_P = g_Q$ for all translation maps τ_P with $P \in E[m]$. But as we have shown, these translation maps are the elements of the Galois group of the extension $k(E)/[m]^*k(E)$ via the map Ξ sending $P \mapsto \tau_P^*$.
- Hence g_Q is Galois-invariant, so it is an element of the base field $[m]^*k(E)$, meaning $g_Q = h \circ [m]$ for some $h \in k(E)$.
- But now $f_Q \circ [m] = g_Q^m = h^m \circ [m]$ so $f_Q = h^m$.
- So $\mathrm{div}(f_Q) = m\mathrm{div}(h)$ so $\mathrm{div}(h) = [Q] - [O]$. Then $[Q] - [O]$ is principal so it resolves to the identity: thus $Q = O$.

The Weil Pairing, VI: But Now You Did VI Twice

4. (Galois-equivariance) If E is defined over F, then for any $\sigma \in \mathrm{Gal}(k/F)$ we have $e_m(\sigma P, \sigma Q) = \sigma[e_m(P, Q)]$.

Proof:

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$ with $g_Q^m = f_Q \circ [m]$.

The Weil Pairing, VI: But Now You Did VI Twice

4. (Galois-equivariance) If E is defined over F, then for any $\sigma \in \mathrm{Gal}(k/F)$ we have $e_m(\sigma P, \sigma Q) = \sigma[e_m(P, Q)]$.

Proof:

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$ with $g_Q^m = f_Q \circ [m]$.
- Then $\mathrm{div}(\sigma f_Q) = m[\sigma Q] - m[O]$ and $\mathrm{div}(\sigma g_Q) = [m]^*\sigma Q - [m]^*O$ and $(\sigma g_Q)^m = (\sigma f_Q) \circ [m]$ since the Galois action carries through on divisors and functions, so we have $f_{\sigma Q} = \sigma f_Q$ and $g_{\sigma Q} = \sigma g_Q$.
- Then $e_m(\sigma P, \sigma Q) = \dfrac{g_{\sigma Q}(X + \sigma P)}{g_{\sigma Q}(X)} = \dfrac{\sigma g_Q(\sigma^{-1}X + P)}{\sigma g_Q(\sigma^{-1}X)} = \sigma \left[\dfrac{g_Q(Y + P)}{g_Q(Y)} \right] = \sigma[e_m(P, Q)]$ where $Y = \sigma^{-1}X$.

The Weil Pairing, VII: We're Just Ignoring Double VI?

5. (Compatibility) For any $P \in E[mm']$ and $Q \in E[m]$ we have $e_{mm'}(P, Q) = e_m([m']P, Q)$.

Proof:

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^* Q - [m]^* O$ with $g_Q^m = f_Q \circ [m]$.

The Weil Pairing, VII: We're Just Ignoring Double VI?

5. (Compatibility) For any $P \in E[mm']$ and $Q \in E[m]$ we have $e_{mm'}(P, Q) = e_m([m']P, Q)$.

Proof:

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$ with $g_Q^m = f_Q \circ [m]$.
- Then $\mathrm{div}(f_Q^{m'}) = mm'[Q] - mm'[O]$ and $(g_Q \circ [m'])^{mm'} = (f_Q \circ [m'])^{m'}$.
- Hence $e_{mm'}(P, Q) = \dfrac{(g \circ [m'])(X + P)}{(g \circ [m'])(X)} = \dfrac{g([m']X + [m']P)}{g([m']X)} = e_m([m']P, Q)$.

The Weil Pairing, VIII: I Guess So, Apparently

6. (Surjectivity) For any mth root of unity ζ_m, there exist $P, Q \in E[m]$ with $e_m(P, Q) = \zeta_m$.

Proof:

The Weil Pairing, VIII: I Guess So, Apparently

6. (Surjectivity) For any mth root of unity ζ_m, there exist $P, Q \in E[m]$ with $e_m(P, Q) = \zeta_m$.

Proof:

- By (1) and (2), the image of $e_m : E[m] \times E[m] \to \mu_m$ is a subgroup of μ_m.
- Suppose the image has order $d|m$. Then for all P and Q we have $e_m(P, Q)^d = 1$, which by (1) says that $e_m(P, [d]Q) = 1$.
- By non-degeneracy, this implies $[d]Q = O$ for all $Q \in E[m]$, which can only happen when $d = m$. Hence e_m is onto.

The Weil Pairing, VIII: I Guess So, Apparently

6. (Surjectivity) For any mth root of unity ζ_m, there exist $P, Q \in E[m]$ with $e_m(P, Q) = \zeta_m$.

Proof:

- By (1) and (2), the image of $e_m : E[m] \times E[m] \to \mu_m$ is a subgroup of μ_m.
- Suppose the image has order $d|m$. Then for all P and Q we have $e_m(P, Q)^d = 1$, which by (1) says that $e_m(P, [d]Q) = 1$.
- By non-degeneracy, this implies $[d]Q = O$ for all $Q \in E[m]$, which can only happen when $d = m$. Hence e_m is onto.

Exercise: Suppose E is defined over F and $E[m] \subseteq E(F)$. Show that F contains the mth roots of unity.

Exercise: Suppose E is defined over $\mathbb{Q}$ and $p > 2$ is a prime. Show that the p-torsion subgroup of $E(\mathbb{Q})$ is either cyclic or trivial.

The Weil Pairing, VI: Oh No, Not A Third One

7. (Adjoints) For any isogeny $\varphi : E_1 \to E_2$ and any $P \in E_1[m]$ and $Q \in E_2[m]$, we have $e_m^{(1)}(P, \hat{\varphi}(Q)) = e_m^{(2)}(\varphi(P), Q)$ where $e_m^{(i)}$ is the Weil pairing on E_i.

Proof:

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^*Q - [m]^*O$ with $g_Q^m = f_Q \circ [m]$.
- First, we want to construct $f_{\hat{\varphi}(Q)}$ and $g_{\hat{\varphi}(Q)}$.

The Weil Pairing, VI: Oh No, Not A Third One

7. (Adjoints) For any isogeny $\varphi : E_1 \to E_2$ and any $P \in E_1[m]$ and $Q \in E_2[m]$, we have $e_m^{(1)}(P, \hat{\varphi}(Q)) = e_m^{(2)}(\varphi(P), Q)$ where $e_m^{(i)}$ is the Weil pairing on E_i.

Proof:

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $\mathrm{div}(g_Q) = [m]^* Q - [m]^* O$ with $g_Q^m = f_Q \circ [m]$.
- First, we want to construct $f_{\hat{\varphi}(Q)}$ and $g_{\hat{\varphi}(Q)}$.
- Observe that $\varphi^*[Q] - \varphi^*[O] - [\hat{\varphi}(Q)] + [O] \in \mathrm{Div}(E_1)$ is principal on E_1 since it has degree 0 and the sum of points resolves to zero, since $\hat{\varphi}(Q)$ is defined to be the sum $\sum_{Q' \in \varphi^{-1}(Q)} Q' - \sum_{R \in \varphi^{-1}(0)} R$ and these are exactly the points in the sum for $\varphi^*[Q]$ and $\varphi^*[O]$ respectively.
- So choose h with $\mathrm{div}(h) = \varphi^*[Q] - \varphi^*[O] - [\hat{\varphi}(Q)] + [O]$.

The Weil Pairing, IV: Okay, Now This Is Just Silly

7. (Adjoints) For any isogeny $\varphi : E_1 \to E_2$ and any $P \in E_1[m]$ and $Q \in E_2[m]$, we have $e_m^{(1)}(P, \hat{\varphi}(Q)) = e_m^{(2)}(\varphi(P), Q)$.

Proof (continued):

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $g_Q^m = f_Q \circ [m]$ and $\mathrm{div}(h) = \varphi^*[Q] - \varphi^*[O] - [\hat{\varphi}(Q)] + [O]$.

The Weil Pairing, IV: Okay, Now This Is Just Silly

7. (Adjoints) For any isogeny $\varphi : E_1 \to E_2$ and any $P \in E_1[m]$ and $Q \in E_2[m]$, we have $e_m^{(1)}(P, \hat{\varphi}(Q)) = e_m^{(2)}(\varphi(P), Q)$.

<u>Proof</u> (continued):

- Take f_Q, g_Q with $\mathrm{div}(f_Q) = m[Q] - m[O]$ and $g_Q^m = f_Q \circ [m]$ and $\mathrm{div}(h) = \varphi^*[Q] - \varphi^*[O] - [\hat{\varphi}(Q)] + [O]$.
- Now, we have $\mathrm{div}(f_Q \circ \varphi) = \varphi^* \mathrm{div}(f_Q) = m\varphi^*[Q] - m\varphi^*[O]$ by properties of φ^*, and so $\mathrm{div}\left[\frac{f_Q \circ \varphi}{h^m}\right] = m[\hat{\varphi}(Q)] - m[O]$, meaning that we may take $f_{\hat{\varphi}(Q)} = \frac{f_Q \circ \varphi}{h^m}$.
- To find a corresponding $g_{\hat{\varphi}(Q)}$ we can observe that

$$f_{\hat{\varphi}(Q)} \circ [m] = \frac{f_Q \circ \varphi}{h^m} \circ [m] = \frac{f_Q \circ [m] \circ \varphi}{h^m \circ [m]} = \frac{g_Q^m \circ \varphi}{h^m \circ [m]} = \left(\frac{g_Q \circ \varphi}{h \circ [m]}\right)^m$$

so we may take $g_{\hat{\varphi}(Q)} = \dfrac{g_Q \circ \varphi}{h \circ [m]}$.

The Weil Pairing, XVI: Wait, Is XVI Actually Correct?

7. (Adjoints) For any isogeny $\varphi : E_1 \to E_2$ and any $P \in E_1[m]$ and $Q \in E_2[m]$, we have $e_m^{(1)}(P, \hat{\varphi}(Q)) = e_m^{(2)}(\varphi(P), Q)$.

Proof (the grand finale):

- We have $f_{\hat{\varphi}(Q)} = \dfrac{f_Q \circ \varphi}{h^m}$ and $g_{\hat{\varphi}(Q)} = \dfrac{g_Q \circ \varphi}{h \circ [m]}$.
- Then $e_m^{(1)}(P, \hat{\varphi}(Q)) = \dfrac{g_{\hat{\varphi}(Q)}(X+P)}{g_{\hat{\varphi}(Q)}(X)}$

$$= \frac{(g_Q \circ \varphi)(X+P)/(h \circ [m])(X+P)}{(g_Q \circ \varphi)(X)/(h \circ [m])(X)}$$

$$= \frac{g_Q(\varphi(X)+\varphi(P))}{g_Q(\varphi(X))} \cdot \frac{h(mX)}{h(mX+mP)}$$

$$= \frac{g_Q(Y+\varphi(P))}{g_Q(Y)} = e_m^{(2)}(\varphi(P), Q) \text{ where } Y = \varphi(X).$$

The Weil Pairing, XVII: Let's Just Say This Is Right

Now that we have given a more natural construction of the Weil pairing on $E[m]$, we can extend this pairing to the Tate module by taking inverse limits.

The Weil Pairing, XVII: Let's Just Say This Is Right

Now that we have given a more natural construction of the Weil pairing on $E[m]$, we can extend this pairing to the Tate module by taking inverse limits.

- Explicitly, for a prime $l \neq \mathrm{char}(k)$, we have a Weil pairing $e_{l^d} : E[l^d] \times E[l^d] \to \mu_{l^d}$.
- The Tate module is formed using the inverse system $E[l] \xleftarrow{[l]} E[l^2] \xleftarrow{[l]} E[l^3] \xleftarrow{[l]} E[l^4] \xleftarrow{[l]} \cdots$.
- The corresponding inverse system on l-power roots of unity is $\mu_l \xleftarrow{l} \mu_{l^2} \xleftarrow{l} \mu_{l^3} \xleftarrow{l} \mu_{l^4} \xleftarrow{l} \cdots$,
  where the map $l : \mu_{l^{d+1}} \to \mu_{l^d}$ is the lth-power map.
- Those certainly look fairly consistent!

The Weil Pairing, XVIII: I'm Fine If You Are

But what does the inverse limit of the groups μ_{l^d} look like?

- By choosing a specific root of unity as generator and making consistent choices the inverse system becomes $\mathbb{Z}/l\mathbb{Z} \xleftarrow{l} \mathbb{Z}/l^2\mathbb{Z} \xleftarrow{l} \mathbb{Z}/l^3\mathbb{Z} \xleftarrow{l} \mathbb{Z}/l^4\mathbb{Z} \xleftarrow{l} \cdots$, which (by using the isomorphism $l\mathbb{Z}/l^{d+1}\mathbb{Z} \cong \mathbb{Z}/l^d\mathbb{Z}$ via dividing representatives by l) is equivalent to our inverse system $\mathbb{Z}/l\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^2\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^3\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^4\mathbb{Z} \xleftarrow{\pi} \cdots$ for $\mathbb{Z}_l$.
- Hence, by selecting consistent choices of generators for the l^d-power roots of unity (i.e., generators $\zeta_1, \zeta_2, \ldots, \zeta_d, \ldots$ with $\zeta_{d+1}^l = \zeta_d$), which is equivalent to selecting a topological generator of μ_{l^∞}, we may view the Weil pairing as taking its values in $\mathbb{Z}_l$.

It remains to show that the inverse-limit structure of $\mathbb{Z}_l$ is consistent with the inverse-limit structure of the Tate module.

The Weil Pairing, XIX

Proposition (Weil Pairing on Tate Module)

Let E/k be an elliptic curve and l be a prime with $l \neq \mathrm{char}(k)$. Then the Weil pairings $e_{l^d} : E[l^d] \times E[l^d] \to \mu_{l^d}$ extend to a pairing $e : T_l[E] \times T_l[E] \to \varprojlim_d \mu_{l^d} \cong \mathbb{Z}_l$.

This l-adic Weil pairing is bilinear, alternating, nondegenerate, Galois-equivariant, and the dual of an isogeny behaves as an adjoint.

Proof:

The Weil Pairing, XIX

Proposition (Weil Pairing on Tate Module)

Let E/k be an elliptic curve and l be a prime with $l \neq \mathrm{char}(k)$. Then the Weil pairings $e_{l^d} : E[l^d] \times E[l^d] \to \mu_{l^d}$ extend to a pairing $e : T_l[E] \times T_l[E] \to \varprojlim_d \mu_{l^d} \cong \mathbb{Z}_l$.

This l-adic Weil pairing is bilinear, alternating, nondegenerate, Galois-equivariant, and the dual of an isogeny behaves as an adjoint.

Proof:

- The Weil pairings e_{l^d} are compatible with the inverse limit $\varprojlim_d \mu_{l^d}$, since by the compatibility and bilinearity properties we have $e_{l^{d+1}}(P, Q)^l = e_{l^d}([l]P, Q)^l = e_l([l]P, [l]Q)$.
- The other properties follow by taking the inverse limit of the properties we showed earlier.

Proving The Weil Conjectures For Elliptic Curves, I

The l-adic Weil pairing provides the final ingredient for proving the Weil conjectures for elliptic curves:

Theorem (Weil Conjectures for Elliptic Curves)

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic p and let φ be the qth-power Frobenius map. Then the following hold:

1. *For any prime $l \neq p$, if ψ_l is the image of φ under the l-adic Galois representation $\rho_l : \mathrm{Gal}(k/F) \to \mathrm{Aut}[T_l(E)]$, then $\det(\psi_l) = \deg \varphi$ and $\mathrm{tr}(\psi_l) = 1 + \deg(\varphi) - \deg(1 - \varphi)$.*
2. *The determinant and trace of ψ_l are integers that are are independent of l, and the characteristic polynomial $\det(T - \psi_l) = T^2 - \mathrm{tr}\psi_l T + \det \psi_l$ has two complex-conjugate roots of absolute value $\sqrt{q}$.*

Proving The Weil Conjectures For Elliptic Curves, II

The l-adic Weil pairing provides the final ingredient for proving the Weil conjectures for elliptic curves:

Theorem (Weil Conjectures for Elliptic Curves, continued)

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic p and let φ be the qth-power Frobenius map. Then the following hold:

3. *For any $n \geq 1$, $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$ for some complex conjugates α and β of absolute value $\sqrt{q}$.*
4. *The zeta function $\zeta_C(T) = \dfrac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$ for some complex conjugates α and β of absolute value $\sqrt{q}$. As an immediate consequence, the Weil conjectures hold for E.*

Proving The Weil Conjectures For Elliptic Curves, III

1. For any prime $l \neq p$, if ψ_l is the image of φ under the l-adic Galois representation $\rho_l : \mathrm{Gal}(k/F) \to \mathrm{Aut}[T_l(E)]$, then $\det(\psi_l) = \deg \varphi$ and $\mathrm{tr}(\psi_l) = 1 + \deg(\varphi) - \deg(1 - \varphi)$.

Proof:

Proving The Weil Conjectures For Elliptic Curves, III

1. For any prime $l \neq p$, if ψ_l is the image of φ under the l-adic Galois representation $\rho_l : \mathrm{Gal}(k/F) \to \mathrm{Aut}[T_l(E)]$, then $\det(\psi_l) = \deg \varphi$ and $\mathrm{tr}(\psi_l) = 1 + \deg(\varphi) - \deg(1 - \varphi)$.

Proof:

- Choose a $\mathbb{Z}_l$-basis $\{v, w\}$ for $T_l(E)$: then the matrix associated to ψ_l with respect to this basis is some 2×2 matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, meaning that $\psi_l(v) = av + cw$ and $\psi_l(w) = bv + dw$.
- Using the l-adic Weil pairing we then have $e(v, w)^{\deg \varphi} = e([\deg \varphi]v, w) = e((\hat{\varphi} \circ \varphi)v, w) = e(\varphi v, \varphi w) = e(av + cw, bv + dw) = e(v, w)^{ad - bc} = e(v, w)^{\det \psi_l}$ using the bilinearity, adjoint, and alternating properties. But now since e is nondegenerate, we must have $\deg \varphi = \det \psi_l$.
- In the same way, $\deg(1 - \varphi) = \det(1 - \psi)$. Finally, $\mathrm{tr}(\psi_l) = 1 + \left|\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right| - \left|\begin{smallmatrix} 1-a & -b \\ -c & 1-d \end{smallmatrix}\right| = 1 + \deg(\varphi) - \deg(1 - \varphi)$.

Proving The Weil Conjectures For Elliptic Curves, IV

2. The determinant and trace of ψ_l are integers that are are independent of l, and the characteristic polynomial $\det(T - \psi_l) = T^2 - \mathrm{tr}\psi_l T + \det \psi_l$ has two complex-conjugate roots of absolute value $\sqrt{q}$.

Proof:

Proving The Weil Conjectures For Elliptic Curves, IV

2. The determinant and trace of ψ_l are integers that are are independent of l, and the characteristic polynomial $\det(T - \psi_l) = T^2 - \mathrm{tr}\psi_l T + \det \psi_l$ has two complex-conjugate roots of absolute value $\sqrt{q}$.

Proof:

- The first part is immediate from (1), since $\deg \varphi$ and $\deg(1 - \varphi)$ are both fixed integers.
- Now, for any rational number m/n, we have $\det(m/n - \psi_l) = \det(m - n\psi_l)/n^2 = \deg(m - n\varphi)/n^2 \geq 0$ since isogenies have nonnegative degree.
- Hence by continuity, the characteristic polynomial $\det(T - \psi_l)$ is nonnegative on $\mathbb{R}$, so it cannot have distinct real roots: thus its roots α and β are complex conjugates (possibly equal), and since their product is $\deg \varphi = q$, each has absolute value $\sqrt{q}$ as claimed.

Proving The Weil Conjectures For Elliptic Curves, V

3. For any $n \geq 1$, $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$ for some complex conjugates α and β of absolute value $\sqrt{q}$.

Proof:

Proving The Weil Conjectures For Elliptic Curves, V

3. For any $n \geq 1$, $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$ for some complex conjugates α and β of absolute value $\sqrt{q}$.

Proof:

- As we noted in our earlier discussion of the Weil conjectures, $P \in E(\overline{\mathbb{F}_{q^n}})$ if and only if $\varphi^n(P) = P$ if and only if $P \in \ker(1 - \varphi^n)$.
- Then since $(1 - \varphi^n)^*\omega = \omega$ the map $1 - \varphi^n$ is separable, so $\#E(\mathbb{F}_{q^n}) = \# \ker(1 - \varphi^n) = \deg(1 - \varphi^n)$.
- Now since φ^n is the q^nth-power Frobenius map, applying (1) to it yields $\deg(1 - \varphi^n) = 1 + \deg(\varphi^n) - \mathrm{tr}(\psi_l^n) = 1 + q^n - \alpha^n - \beta^n$ for some complex conjugates α and β of absolute value $\sqrt{q}$.

Proving The Weil Conjectures For Elliptic Curves, VI

4. The zeta function $\zeta_C(T) = \dfrac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$ for some complex conjugates α and β of absolute value $\sqrt{q}$. As an immediate consequence, the Weil conjectures hold for E.

Proof:

Proving The Weil Conjectures For Elliptic Curves, VI

4. The zeta function $\zeta_C(T) = \dfrac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$ for some complex conjugates α and β of absolute value $\sqrt{q}$. As an immediate consequence, the Weil conjectures hold for E.

Proof:

- By definition and (2), we have $\ln \zeta_C(T)$
$$= \sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}$$
$$= \sum_{n=1}^{\infty} (1^n + q^n - \alpha^n - \beta^n) \frac{T^n}{n}$$
$$= -\ln(1-T) - \ln(1-qT) + \ln(1-\alpha T) + \ln(1-\beta T).$$
- Exponentiating yields $\zeta_C(T) = \dfrac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$.

Summary

We introduced the Weil pairing and established many of its properties.

We used the properties of the Weil pairing to prove the Weil conjectures for elliptic curves.

Next lecture: The endomorphism ring.