Week 5

Weil pairing, André Weil (French), 1940.

The Weil pairing is a bilinear map

\[ e: E[\mathbb{Q}] \times E[\mathbb{Q}] \rightarrow \mu_n \subset \overline{\mathbb{Q}} \]

bilinear on the left and right:

\[ e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q) \]
\[ e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2) \]

addition on the curve in \( E[\mathbb{Q}] \) becomes multiplication in \( \mu_n \subset \overline{\mathbb{Q}} \).

\( \overline{\mathbb{Q}} \) is the algebraic closure of the field \( \mathbb{Q} \).

\( E[\mathbb{Q}] \) is the group of the points of order \( n \), or the \( n \)-torsion points, over \( \mathbb{Q} \).

\[ E[\mathbb{Q}] = \{ P \in E \mid nP = 0 \} = \{ P \in E(\overline{\mathbb{Q}}), \; EnP = 0 \} \]

including 0.

Recall that \( E[\mathbb{Q}] \) is isomorphic to \( \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \), and \( \# E[\mathbb{Q}] = n^2 \).

Thus, \( \overline{\mathbb{Q}} \) is the algebraic closure of \( \mathbb{Q} \).

The Weil pairing satisfies

\[ e(P, P) = 1. \]

This pairing can be used to know if two points of order \( n \) are in the same cyclic subgroup or not. Indeed, from \( e(P, P) = 1 \), we deduce \( e(P, P + P) = 1 \), etc...

\[ e(P, aP) = 1 \] for any \( a \neq 0 \). If \( a = \lambda P \) for some \( \lambda \), then \( e(P, aP) = 1. \)

What is \( \mu_n \)? This is the multiplicative group of the \( n \)-th roots of unity.

\[ \mu_n = \{ \zeta \in \overline{\mathbb{Q}}, \; \zeta^n = 1 \} \]

Example: \( K = \mathbb{Q} \), \( \mu_4 = \{ 1, i \} \), \( \mu_2 = \{ 1, -1 \} \), \( \mu_6 = \{ 1, w, w^2 \} \) with \( w = \frac{-1 + \sqrt{-3}}{2} \),

\[ \mu_4 = \{ 1, -1, i, -i \} \] with \( i^2 = -1 \), \( \mu_6 = \{ 1, -1, w, w^2, -w, -w^2 \} \).

If \( n \) \# \( E(\mathbb{F}_p) \), then a first dimension of the \( n \)-torsion is in \( E(\mathbb{F}_p): E(\mathbb{F}_p)[n] \).

\[ E(\mathbb{F}_p)[n] = \{ P \in E(\mathbb{F}_p), \; nP = 0 \} \] over the finite field \( \mathbb{F}_p \).

We need an extension for the other dimension, the \( \infty \)-points of \( n \)-torsion.
EMBEDDING DEGREE

\[ y^2 = x^3 + Ax + B \] is an elliptic curve defined over \( \mathbb{F}_p \).

Let \( r \) a divisor of \( \text{#} E(\mathbb{F}_p) \), \( r^2 \) does not divide \( \text{#} E(\mathbb{F}_p) \),  
the rank \( r \) is prime.

The pairing is \( e : E(\mathbb{F}_p)[r] \times E[1] \to \mu_r \subset \mathbb{F}_p^\times \)

we know we can find \( r \)-torsion points over \( \mathbb{F}_p \)
find \( \mu_r \)-torsion points we don't know, we need an extension of \( \mathbb{F}_p \)

Let \( k \) be the smallest integer such that \( \mu_r \subset \mathbb{F}_{p^k} \).
\( k \) is the order of \( p \mod r \).
\( r \mid p^k - 1 \).

**Notation:** \( \mathbb{F}_p \) is the field of \( p \) elements where \( p \) is prime.
\( \mathbb{F}_p^\times \) or \( \mathbb{F}_p^\ast \) is the multiplicative group of \( \mathbb{F}_p \), or the (multiplicative) group of invertible elements, that is \( \mathbb{F}_p \) minus zero: \( \mathbb{F}_p \lessdot \{0\} \).

\[ \Rightarrow \text{#} \mathbb{F}_p^\times = p - 1 \] (all non-zero elements: \( 1, 2, 3, \ldots, p - 1 \)).

\( \mathbb{F}_p^2 \) is the field of \( p^2 \) elements, this is not "modulo \( p^2 \)" this is: modulo \( p \) and modulo a quadratic irreducible polynomial, for example:

\[ \mathbb{F}_p^2 = \mathbb{F}_p [x] / (x^2 + 1) \] if \( p \equiv 3 \mod 4 \) : analogy with \( \mathbb{Q}(i) \), \( i^2 = -1 \).

\[ \mathbb{F}_p^2 = \mathbb{F}_p \lessdot \{0\} \] is the multiplicative group of invertible elements.
and \( \text{#} \mathbb{F}_p^2 = p^2 - 1 \).

\( \mathbb{F}_p^{x^k} \) is a degree \( k \) extension of \( \mathbb{F}_p \), where \( \mathbb{F}_p^{x^k} = [\mathbb{F}_p[x] / (x^{p^k} + a_{p^k} x + a_0)] \)

\[ \mathbb{F}_p^{x^k} = \{ b_0 + b_1 x + \ldots + b_{p^k - 1} x^{p^k - 1}, b_i \in \mathbb{F}_p, \text{ and } a_0 + a_1 x + \ldots + a_{p^k - 1} x^{p^k - 1} + x^{p^k} = 0 \} \]

\( f(x) = 0 \)

\[ \Rightarrow \text{#} \mathbb{F}_p^{x^k} = p^k, \]
\[ \text{#} \mathbb{F}_p^{x^k} = p^k - 1. \]
Theorem 1: Let \( E \) be an elliptic curve defined over a field \( F_q \) (finite field) and suppose that \( p \) is a prime that divides \( N = \# E(F_q) \) but does not divide \( q - 1 \). Let \( \ell = q - 1 \). Then \( E(F_q^\ell) \) contains \( \ell^2 \) points of order \( \ell \) if \( \ell \mid q^{k-1} \).

Theorem 2: About the chance for \( \ell \) to be "small.

Let \((p, E)\) be a randomly chosen pair consisting of a prime in the interval \( \frac{M}{2} \leq p \leq M \) and an elliptic curve defined over \( F_p \) having a prime number \( \ell \) of points. The probability that \( \ell \mid p^{k-1} \) for some \( \ell \leq (\log p)^2 \) is less than

\[
\frac{c_3}{M} \left( \log M \right)^3 \left( \log \log M \right)^2
\]

for an effectively computable positive constant \( c_3 \).

In other words, curves with small enough \( \ell \leq (\log p)^2 \) are extremely rare. If \( \ell \) is fixed, the expected number of pairs \((q, E)\) where \( q \) is a prime (or primepower) in the range \( \frac{M}{2} \leq q \leq M \) and \( E \) is an elliptic curve over \( F_q \) such that \( E(F_q) \) has a large subgroup with embedding degree \( \ell \), is \( O(M^{1/2+\varepsilon}) \).

We cannot expect to find them by choosing curves at random.

Above on the embedding degree.

- \( \ell \) is the smallest integer such that \( \mu_n \mid E_{F_k} \).
- In the case where \( p \) is prime, it corresponds to
  \( n \mid \Phi_k(p) \) and \( n \mid \Phi_i(p) \) for all \( 1 \leq i \leq k - 1 \),
  where \( \Phi_k \) is the \( k \)-th cyclotomic polynomial.

\[
\Phi_k(x) = \prod_{\zeta \text{ a primitive } k\text{-th root of unity}} (x - \zeta_k)
\]

\( x^{k-1} = \prod_{\text{in } \Phi_{k-1} \text{ including } \zeta_k} \Phi_d(x) \).
Weil pairing and Tate pairing.

\[ e_w : E[n] \times E[n] \to \mu_n \subset \overline{K} \]
\[ (p, q) \mapsto e_w(p, q) \]

\[ e_T : E(F_q)[n] \times E(F_q)[n] \to E(F_q)[n] / E(F_q)[n] \sim \overline{E}_{F_q}^x / (\overline{E}_{F_q}^x)^n \]

Equivalence class

Chapter 11: divisors.

A divisor on an elliptic curve \( E \) defined over a field \( K \) is a formal sum of points

\[ D = \sum a_i (P_i), \quad a_i \in \mathbb{Z} \]

where the \( (P_i) \) are "symbols" of points \( P_i \) and only a finite number of \( a_i \) are non-zero, i.e. the sum is finite.

We can give a structure, and define

\[ D_1 + D_2 = \sum (a_i + a_i') (P_i) \]

just add the multiplicity of the points, where \( (P_i) \) are in \( D_1 \) or \( D_2 \).

Degree:

\[ \deg \left( \sum a_i (P_i) \right) = \sum a_i \in \mathbb{Z} \to \text{sum of the multiplicities, can be } 0, \text{ a negative or positive}. \]

Sum:

\[ \text{sum} \left( \sum a_i (P_i) \right) = \sum a_i P_i \in \overline{E}(\overline{K}) \]

Zero:

\( \text{Div}^0(E) \), the subgroup of divisors of degree 0.

\text{Sum is a surjective morphism: } \text{Div}^0(E) \to \overline{E}(\overline{K}).

That is, any point \( P \in \overline{E}(\overline{K}) \) can be associated to the degree 0 divisor \( (P) - (O) \) where \( O \) is the point at infinity,

\[ \deg (P) - (O) = 0 \text{ and sum } (P) - (O) = P - O = P. \]

Kernel of \( \text{SUM} \): on which set of points do we have \( \sum a_i P_i = O? \)

Example: a line through three points

\[ D = (P) + (Q) + (-P - Q) \text{ has sum } 0 \]

But degree 3 →

\[ D^0 = (P) + (Q) + (-P - Q) - 3 O \text{ has sum } 0 \text{ and degree } 0. \]
Remember the proof of associativity with Bezout's Theorem.

We defined a function

\[ C_A = \frac{P + A}{P + R} - \frac{Q + R}{Q + A} - \frac{P + Q + R}{P + A + R} \]

we can find the exponents of degree 0:

\[ l_{P,Q} \sim \frac{(P) + (Q) + (-P-Q)}{(-3)} \]
\[ l_{Q+R} \sim \frac{(Q+R) + (-Q-R)}{(-2)} \]
\[ l_{P+Q} \sim \frac{(P+Q) + (R) + (-P+Q-R)}{(-3)} \]

Then a degree 0 divisor of \( C_A \) is the formal sum of the divisors of the lines:

\[ D_{C_A} = (P) + (Q) + (-P-Q) + (Q+R) + (-Q-R) + (P+Q) + (R) + (-P+Q-R) \]

and sum (\( D_{C_A} \)) = 0.

In affine coordinates, \( l_{P,Q}(x,y) = \lambda(x-x_0) - \frac{y-y_0}{y_0-x_0}(x-x_0) \), \( \lambda = \frac{x-x_0}{y-y_0} \).

But in projective coordinates, there is a denominator Z.

\[ l_{P,Q}(x,y,z) = \lambda \left( \frac{x-x_0}{z} - x_0 \right) - \left( \frac{y-y_0}{z} - y_0 \right) \]

A zero of a function is a point \( P \in E(K) \) such that \( f(P) = 0 \). (f vanishes at P).

A pole of a function is a point \( P \in E(K) \) at which the denominator of \( f \) vanishes.

\( f(P) = \infty \).

More precisely, we will need the order of the zero and poles.

We know that a tangent at \( P \) to the curve has intersection multiplicity 2 at \( P \) (lecture 1, addition law).

It is possible to have functions with zeros and poles of some multiplicity (order) greater than 1. The divisor of a function \( f \neq 0 \) is \( \text{div}(f) = \sum \text{ord}_P(f)(P) \) \( P \in \text{Div}(E) \).

The divisor of a function is a principal divisor. \( P \in E(K) \) \( a \in k \) such that \( a \cdot P \) is a zero or pole.

**Proposition 11.1 and Theorem 11.2.**

**Prop.** Let \( E \) be an elliptic curve and let \( f \) be a function on \( E \) that is not identically 0.

1. \( f \) has only finitely many zeros and poles.
2. \( \text{deg} \left( \text{div}(f) \right) = 0 \)
3. If \( f \) has no zeros or poles (so \( \text{div}(f) = 0 \)), then \( f \) is a constant.

**Th.** Let \( E \) be an elliptic curve. Let \( D \) be a divisor on \( E \) with \( \text{deg}(D) = 0 \). Then there is a function \( f \) on \( E \) with \( \text{div}(f) = D \) if and only if \( \text{sum}(D) = 0 \).
Continuing the example with the lines. Washington p 342-343.

Let \( P_1, P_2, P_3 \) three points of intersection of a line \( L \) with \( E \).

\[
f(x,y) = ax + by + c \quad \text{is the line equation.}
\]

\[
\text{div}(f) = (P_1) + (P_2) + (P_3) - 3(0)
\]

Now we "add" the vertical line. We "add" the divisors and multiply the function.

\[
v(x,y) = x - x_3 \quad \text{is the equation of the vertical at } P_3.
\]

Its divisor is \( \text{div}(v_{P_3}) = (P_3) + (-P_3) - 2(0) \).

\[
\text{div}
\left( \frac{L_{P_1P_2}}{v_{P_3}} \right) = \text{div}
\left( \frac{ax+by+c}{x-x_3} \right) = \text{div}(L_{P_1P_2}) - \text{div}(v_{P_3}) = (P_1) + (P_2) + (P_3) - 3(0)
\]

\[
- (P_3) - (-P_3) + 2(0)
\]

\[
= (P_1) + (P_2) - (P_3) - 0
\]

and we can check that its sum is \( P_1 + P_2 + P_3 = P_1 + P_2 + (-P_1 - P_2) = 0 \) and has degree 0.

\( P_1 + P_2 = -P_3 \) on \( E \), and

\[
(P_1) + (P_2) = (P_1 + P_2) + 0 + \text{div}
\left( \frac{L_{P_1P_2}}{v_{P_1P_2}} \right)
\]

we will use this result in Weil's algorithm.

On our way to define the Weil pairing, we need:

Let \( T \in E[m] \). There exists a function \( f \in \mathcal{O}_E \) such that

\[
\text{div}(f) = m(T) - m(0) \quad \text{pols of order } n \text{ at } 0, \text{ zeros of order at } T.
\]

Let \( T' \) be a preimage of \( T \) under \( [n] \), that is \([n] T' = T\) \( (T' \text{ is of order } n^2)\).

There is a function \( g \) on \( E \) such that

\[
\text{div}(g) = \sum_{R_i \in E[n^3]} (T' + R_i) - (R_i) = \text{formal sum of the preimage points of } T
\]

under \([n]\) minus the formal sum of points of order \( n \) (preimages of \([n]\) under \([1]\)).

\[
= [n]^*([T]) - [n]^*([0]) \quad (Eulerian, 6.4, 11.6).
\]

\[
\text{div}(g) = (T' + R_1) + (T' + R_2) + (T' + R_3) + \ldots + (T' + R_{m^2})
\]

\[
- (R_1) - (R_2) - (R_3) - \ldots - (R_{m^2})
\]

\( g \) has \( m^2 \) distinct zeros at \( T' + R_i \) and \( m^2 \) distinct poles at \( R_i \); \( R_i \) enumerating the \( m^2 \) points of \([n]\).

Now consider \( f \circ [n] \). The zeros are one point \( S \) such that \( f([n]S) = 0 \), these \( S \) are exactly the \( T' + R_i \). Proof:

The \( T' + R_i \) are zeros of \( n \) of \( f \circ [n] \).

\[
\text{div} \left( f \circ [n] \right) = -m \text{div}(g) \quad \rightarrow \text{up to pull-by-a constant of } K^*, \quad f \circ [n] = g^m.
\]

Now take \( S \in E[n] \), for any \( X \in E \), \( g(X+S)^m = f([n]X + [n]S) = f([n]X) = g(X)^m \).

\( g(X+S)/g(X) \) is not \( n \)th of \( f \).
Miller algorithm.

How to compute the function $f$ such that $\text{div}(f) = n(P) - n(0) = \text{PE}[n]$.

Double- and add. Let $P \in \text{PE}[n]$.

Let $f_i$ a function of division $\text{div}(f_i) = i(P) - (i + j_i)P - (i - 1)Q$.

Then $f_n = n(P) - (n)P - (n - 1)Q = n(P) - n(0)$ because $(n)P = 0$.

$$\text{div}(f_n) = \text{div}(f).$$

$$\text{div}(f_{i+j}) = (i+j)(P) - (i+j+1)P - (i+j-1)Q$$

$$= (i)(P) - (i-1)Q + (j)(P) - (j-1)Q - (i+j)P - (i-1)Q$$

$$\text{div}(f_{i-j}) = \text{div}(f_i) - \text{div}(f_j).$$

$$\text{div}(f_{i+j}) = \text{div}(f_i) + \text{div}(f_j) + \text{div}(f_{i-j}).$$

$$\text{div}(f_{i+j}) = f_i + f_j - \frac{\ell_{i+j}P}{\ell_{i+j}P}.$$  

$$f_{i+1} = f_i + \frac{\ell_{i+1}P}{\ell_{i+1}P},$$  

where $\ell_{i+1}P$ is the tangent at $iP$, $v_{i+1}P$ is the line through $iP$ and $P$, $v_{i+1}P$ is the line through $iP$ and $P$.

Miller algorithm.

Length of the FOR loop: $\log_2 n$.

big problem: this is a function whose coefficients and degrees of numerator and denominator grow very fast.

Solution: evaluate the function at a point at each step.