01-03-2022 Part 2. Pairings. Week 5

Weil pairing, André Weil (French), ≃1940.

The Weil pairing is a bilinear map

$$e : E[n] \times E[n] \longrightarrow \mu_n \subset \overline{K}$$

bar means the algebraic closure, that is any extension

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 $E[n]$ becomes multiplication in $\mu_n \subset \overline{K}$.

$\overline{K}$ is the algebraic closure of the field K.

$E[n]$ is the group of the points of order n, or the n-torsion points, over $\overline{K}$.

$$E[n] = \{ P \in E, \ (x,y) \in \overline{K} \times \overline{K} : y^2 = x^3+ax+b \text{ and } [n]P = \mathcal{O}\} \cup \{\mathcal{O}\}.$$
$$= \{ \underbrace{P \in E}_{\text{including } \mathcal{O}}, \ [n] P = \mathcal{O} \} = \{ P \in E(\overline{K}), \ [n] P = \mathcal{O} \}$$

Recall that $E[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, and $\# E[n] = n^2$.
over $\overline{K}$ the algebraic closure (n coprime to char(K)).

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 $Q = \lambda P$ for some λ, then $e(P,Q) = 1$.

What is μ_n? This is the multiplicative group of the n-th roots of unity.

$$\boxed{\mu_n = \{ x \in \overline{K}, \ x^n = 1 \}.}$$

example: $K = \mathbb{C}$, $\mu_1 = \{1\}$, $\mu_2 = \{1, -1\}$, $\mu_3 = \{1, \omega, \omega^2\}$ with $\omega = \frac{-1+\sqrt{-3}}{2}$,
$\mu_4 = \{1, -1, i, -i\}$ with $i^2 = -1$, $\mu_6 = \{1, -1, \omega, \omega^2, -\omega, -\omega^2\}$.

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

$E(\mathbb{F}_p)[n] = \{ P \in E(\mathbb{F}_p), \ [n] P = \mathcal{O} \}$. There we explicit the field: $\mathbb{F}_p$.

We need an extension for the other dimension, the other points of n-torsion.

EMBEDDING DEGREE

$E: y^2 = x^3 + Ax + B$ an elliptic curve defined over $\mathbb{F}_p$.
Let r a divisor of $E(\mathbb{F}_p)$, r^2 does not divide $\#E(\mathbb{F}_p)$: $r^2 \nmid \#E(\mathbb{F}_p)$,
then r is prime.

The pairing is $e: \underbrace{E(\mathbb{F}_p)[r]}_{\text{we know we can find r-torsion points over } \mathbb{F}_p} \times \underbrace{E[r]}_{\text{for the second dimension, we don't know, we need an extension of } \mathbb{F}_p} \longrightarrow \mu_r \subset \overline{\mathbb{F}_p}$

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 $\mathbb{F}_p^*$ is the multiplicative group of $\mathbb{F}_p$, or the (multiplicative) group of invertible elements, that is $\mathbb{F}_p$ minus zero: $\mathbb{F}_p \setminus \{0\}$.

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

$\mathbb{F}_{p^2}$ 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:

$\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X]/(X^2+1)$ if $p \equiv 3 \bmod 4$. analogy with $\mathbb{Q}(i)$, $i^2 = -1$.
$\simeq \{ a + bx,\ a, b \in \mathbb{F}_p,\ x^2 = -1 \}$.

$\mathbb{F}_{p^2}^\times = \mathbb{F}_{p^2} \setminus \{0\}$ is the multiplicative group of invertible elements,
and $\# \mathbb{F}_{p^2}^\times = p^2 - 1$.

... $\mathbb{F}_{p^k}$ is a degree-k extension of $\mathbb{F}_p$, where $\mathbb{F}_{p^k} = \mathbb{F}_p[X]/(X^k + \dots + a_1 X + a_0)$ a monic irreducible polynomial of degree k

$= \{ b_0 + b_1 x + \dots + b_{k-1} x^{k-1},\ b_i \in \mathbb{F}_p, \text{ and } \underbrace{a_0 + a_1 x + \dots + a_{k-1} x^{k-1} + x^k = 0}_{f(x) = 0} \}$

$\rightarrow \# \mathbb{F}_{p^k} = p^k$,
$\# \mathbb{F}_{p^k}^\times = p^k - 1$.

01.03.2022 Part 2. Week 5.

BALASUBRAMANIAN - KOBLITZ

Journal of Cryptology, 1998, volume 11, p. 141-145.

Theorem 1: Let E be an elliptic curve defined over a field $\mathbb{F}_q$ (finite field) and suppose that ℓ is a prime that divides $N = \# E(\mathbb{F}_q)$ but does not divide $q-1$: $\ell \nmid q-1$. Then $E(\mathbb{F}_{q^k})$ contains ℓ^2 points of order ℓ iff $\ell \mid q^k - 1$.

Theorem 2: about the chances for k to be "small".

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

$$c_3 \frac{(\log M)^9 (\log \log M)^2}{M}$$

for an effectively computable positive constant c_3.

In other words, curves with small enough $k \lesssim (\log p)^2$ are extremely rare.

If k is fixed, the expected number of pairs (q, E) where q is a prime (or prime power) in the range $M/2 \leq q \leq M$ and E is an elliptic curve over $\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ has a large subgroup with embedding degree k, is $O(M^{1/2+\varepsilon})$.

$\rightarrow$ we cannot expect to find them by choosing curves at random.

More on the embedding degree.

- k is the smallest integer such that $\mu_n \subset \mathbb{F}_{p^k}$.
- in the easier case where p is prime, it corresponds to

$$n \mid \Phi_k(p) \quad \text{and} \quad n \nmid \Phi_i(p) \text{ for all } 1 \leq i \leq k-1.$$

where Φ_k is the k-th cyclotomic polynomial.

$$\phi_k(x) = \prod_{\substack{\zeta \text{ a primitive} \\ k\text{-th root of} \\ \text{unity}}} (x - \zeta_k) \qquad \text{and} \qquad x^k - 1 = \prod_{\substack{d \mid k \\ \text{including} \\ 1 \text{ and } k}} \phi_d(x).$$

Weil pairing and Tate pairing

$$e_W : E[n] \times E[n] \longrightarrow \mu_n \subset \overline{K}$$
$$(P, Q) \longmapsto e_W(P, Q)$$

$$e_T : \underbrace{E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k}) / n E(\mathbb{F}_{q^k})}_{\text{equivalence class}} \longrightarrow \underbrace{\mathbb{F}_{q^k}^{\times} / (\mathbb{F}_{q^k}^{\times})^n}_{\text{equivalence class}}$$

Chapter 11: divisors.

A DIVISOR on an elliptic curve E defined over a field K is a FINITE FORMAL SUM OF POINTS

$$D = \sum_i a_i (P_i), \quad a_i \in \mathbb{Z}.$$ where the (P_i) are "symbols" of points P_i and the a_i are the multiplicities of symbols (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

$$D_1 + D_2 = \sum_i (a_i + a_i')(P_i)$$ → just add the multiplicities of the points, where (P_i) are in D_1 or D_2.

DEGREE: $\deg\left(\sum_i a_i (P_i)\right) = \sum_i a_i \in \mathbb{Z}$ → sum of the multiplicities, can be 0, a negative (positive).

SUM: $\mathrm{sum}\Big(\underbrace{\sum_i a_i (P_i)}_{\text{a formal sum of points of } E(\overline{K})}\Big) = \underbrace{\sum_i a_i P_i}_{\text{the arithmetic sum of points on } E(\overline{K}) \text{ with the addition law on } E} \in E(\overline{K})$

$\mathrm{Div}^0(E)$: the subgroup of divisors of degree 0. (zero)

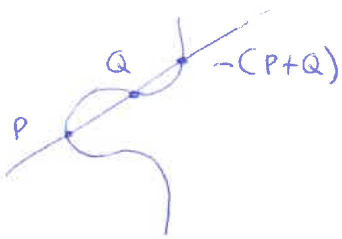
SUM is a surjective morphism: $\mathrm{Div}^0(E) \to E(\overline{K})$.

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

$$\deg((P) - (\mathcal{O})) = 0 \quad \text{and} \quad \mathrm{sum}((P) - (\mathcal{O})) = P - \mathcal{O} = P.$$

Kernel of SUM: on which set of points do we have $\sum_i a_i P_i = \mathcal{O}$?

Example: a line through three points



$D = (P) + (Q) + (-P-Q)$ has sum 0

but degree 3 →

$D^0 = (P) + (Q) + (-P-Q) - 3\,\mathcal{O}$

has sum 0 and degree 0.

Remember the proof of associativity with Bézout's theorem.

We defined a function

$$\mathcal{C}_1 = \underbrace{l_{P,Q}}_{(P)+(Q)+((-P-Q))} \cdot \underbrace{v_{Q+R}}_{(Q+R)+(-Q-R)+(\mathcal{O})} \cdot \underbrace{l_{P+Q,R}}_{(P+Q)+(R)+(-(P+Q)-R)}$$

we can find three divisors of degree 0:

$$l_{P,Q} \longleftrightarrow (P)+(Q)+(-P-Q)\ -3\mathcal{O}$$

$$v_{Q+R} \longleftrightarrow (Q+R)+(-Q-R)\ -2\mathcal{O}$$

$$l_{P+Q,R} \longleftrightarrow (P+Q)+(R)+(-(P+Q)-R)\ -3\mathcal{O}$$

where does this $\mathcal{O}$ come from?

then a degree 0 divisor of $\mathcal{C}_1$ is the formal sum of the divisors of the lines:

$$D_{\mathcal{C}_1} = (P)+(Q)+(-P-Q)+(Q+R)+(-Q-R)+(P+Q)+(R)+(-(P+Q)-R)-8\mathcal{O}.$$

and $\mathrm{sum}(D_{\mathcal{C}_1}) = \mathcal{O}$.

in affine coordinates, $l_{P,Q}(x,y) = \lambda(x-x_0)-(y-y_0)$, $\lambda = \cancel{\dfrac{x_1-x_0}{y_1-y_0}}$ and $\begin{cases} P(x_0,y_0) \\ Q(x_1,y_1) \end{cases}$

$$\lambda = \frac{y_1-y_0}{x_1-x_0}$$

but in PROJECTIVE coordinates, there is a denominator Z.

$$l_{P,Q}(X,Y,Z) = \lambda\left(\frac{X}{Z}-x_0\right)-\left(\frac{Y}{Z}-y_0\right)$$

A ZERO of a function is a point $P \in E(\bar{K})$ s. that $f(P)=0$. (f vanishes at P).

A POLE of a function is a point $P \in E(\bar{K})$ at which the denominator of f vanishes: $f(P)=\infty$.

More precisely we will need the order of the zeros and poles.

We saw 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 $\mathrm{div}(f) = \sum_{P \in E(\bar{K})} \underbrace{\mathrm{ord}_P(f)}_{a_i = \text{order of } P \text{ at which } f \text{ vanishes, } >0 \text{ for zeros, } <0 \text{ for poles}} (P) \in \mathrm{Div}(E)$. (P): symbol (P).

The divisor of a function is a PRINCIPAL divisor.

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. $\deg(\mathrm{div}(f)) = 0$
3. if f has no zeros or poles (so $\mathrm{div}(f)=0$), then f is a constant.

TH. Let E be an elliptic curve. Let D be a divisor on E with $\deg(D)=0$. Then there is a function f on E with $\mathrm{div}(f)=D$ if and only if $\mathrm{sum}(D)=\infty$.

Continuing the example with the lines. Washington p 342-343.

Let P_1, P_2, P_3 three distinct points of intersection of a line ℓ with E.

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

$$\mathrm{div}(f) = (P_1) + (P_2) + (P_3) - 3\,\mathcal{O}$$

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

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

its divisor is $\mathrm{div}(v_{P_3}) = (P_3) + (-P_3) - 2\mathcal{O}$

$$\mathrm{div}\left(\frac{\ell_{P_1,P_2}}{v_{P_3}}\right) = \mathrm{div}\left(\frac{ax+by+c}{x-x_3}\right) = \mathrm{div}(\ell_{P_1,P_2}) - \mathrm{div}(v_{P_3}) = (P_1)+(P_2)+(P_3) - 3\mathcal{O} - (P_3) - (-P_3) + 2\mathcal{O}$$

$$= (P_1) + (P_2) - (-P_3) - \mathcal{O}$$

and we can check that is sums to $P_1 + P_2 + P_3 = P_1 + P_2 + (-P_1 - P_2) = \mathcal{O}$ and has degree 0.

$P_1 + P_2 = -P_3$ on E, and

$$(P_1) + (P_2) = (P_1 + P_2) + \mathcal{O} + \mathrm{div}\left(\frac{\ell_{P_1,P_2}}{v_{P_1+P_2}}\right)$$

we will use this result in Miller's algorithm.

On our way to define the Weil pairing, we need: $\boxed{\text{11.2 in the book}}$.

Let $T \in E[n]$. There exists a function f on E such that

$$\mathrm{div}(f) = n(T) - n(\mathcal{O}) \qquad \text{pole of order } n \text{ at } \mathcal{O}\text{, zero of order } n \text{ at } T.$$

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

There is a function g on E such that

$$\mathrm{div}(g) = \sum_{R_i \in E[n]} (T' + R_i) - (R_i)$$

= formal sum of the preimage points of T under $[n]$, minus the formal sum of points of order n (preimages of $\mathcal{O}$ under $[n]$)

$$= [n]^*(T) - [n]^*(\mathcal{O}) \quad (\text{Silverman, } 6.4,\ \text{III}.6).$$

$$\mathrm{div}(g) = (T' + R_1) + (T' + R_2) + (T' + R_3) + \dots + (T' + R_{n^2}) - (R_1) - (R_2) - (R_3) - \dots - (R_{n^2})$$

$m = n$

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 $E[m]$.

Now consider $f \circ [m]$. The zeros are are points S such that $f([m]S) = \mathcal{O}$, these S are exactly the $T' + R_i$ zeros of g.

The $T' + R_i$ are zeros of order n of $f \circ [n]$.

$\mathrm{div}(f \circ [n]) = m\,\mathrm{div}(g)$. $\to$ up to mult by a constant of $\bar{K}^*$, $f \circ [m] = g^m$.

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

$\to g(X+S)/g(X)$ is an m-root of unity.

Miller algorithm.

Victor Miller, Short programs for functions on curves, 1986.
1947 – USA. 1978 – 1993 IBM. 1993 – 2022: inst. def. Anal. now at Meta Platforms.

How to compute the function f such that $\mathrm{div}(f) = n(P) - n(\mathcal{O})$? $P \in E[n]$.

Double-and add. Let $P \in E[n]$.

Let f_i a function of divisor $\mathrm{div}(f_i) = i(P) - (\underbrace{[i]P}_{\text{the point } [i]P \text{ on } E.}) - (i-1)\mathcal{O}$. principal divisor of degree 0.

Then $\mathrm{div}(f_n) = n(P) - ([n]P) - (n-1)\mathcal{O} = n(P) - n(\mathcal{O})$ because $[n]P = \mathcal{O}$.

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

$$\begin{aligned}\mathrm{div}(f_{i+j}) &= (i+j)(P) - ([i+j]P) - (i+j-1)\mathcal{O} \\ &= (i)(P) - (i-1)\mathcal{O} + (j)(P) - (j-1)\mathcal{O} - ([i+j]P) - \mathcal{O} \\ &= \underbrace{i(P) - ([i]P) - (i-1)\mathcal{O}}_{\mathrm{div}(f_i)} + \underbrace{j(P) - ([j]P) - (j-1)\mathcal{O}}_{\mathrm{div}(f_j)} + \underbrace{([i]P) + ([j]P) - ([i+j]P) - \mathcal{O}}\end{aligned}$$

is the divisor of the line $\ell_{[i]P,[j]P}$ divided by the vertical $v_{[i+j]P}$.

$$\mathrm{div}(\ell_{[i]P,[j]P}) = ([i]P) + ([j]P) + (-[i+j]P) - 3\mathcal{O}$$
$$\mathrm{div}(v_{[i+j]P}) = ([i+j]P) + (-[i+j]P) - 2\mathcal{O}$$

$$\mathrm{div}(f_{i+j}) = \mathrm{div}(f_i) + \mathrm{div}(f_j) + \mathrm{div}(\ell_{[i]P,[j]P}) - \mathrm{div}(v_{[i+j]P})$$

Hence $f_{i+j} = f_i \cdot f_j \cdot \ell_{[i]P,[j]P} / v_{[i+j]P}$

$f_{2i} = f_{i+i} = f_i^2 \dfrac{\ell_{iP,iP}}{v_{2iP}}$ where $\ell_{iP,iP}$ is the tangent at iP, v_{2iP} vertical at $[2i]P$.

$f_{i+1} = f_i f_1 \dfrac{\ell_{iP,P}}{v_{[i+1]P}}$, $\ell_{iP,P}$ the line through iP and P, $v_{(i+1)P}$ vertical at $[i+1]P$.

$n = \sum_{i=0}^{I-1} b_i 2^i$
$R \leftarrow P$
$f \leftarrow 1$
for $i = I-1$ to 0 by -1 do
  $f \leftarrow f^2\, \ell_{R,R} / v_{2R}$
  $R \leftarrow 2R$
  if $b_i = 1$ then
    $f \leftarrow f \cdot \ell_{R,P} / v_{R+P}$
    $R \leftarrow R+P$
return f

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 $\hookrightarrow Q$.