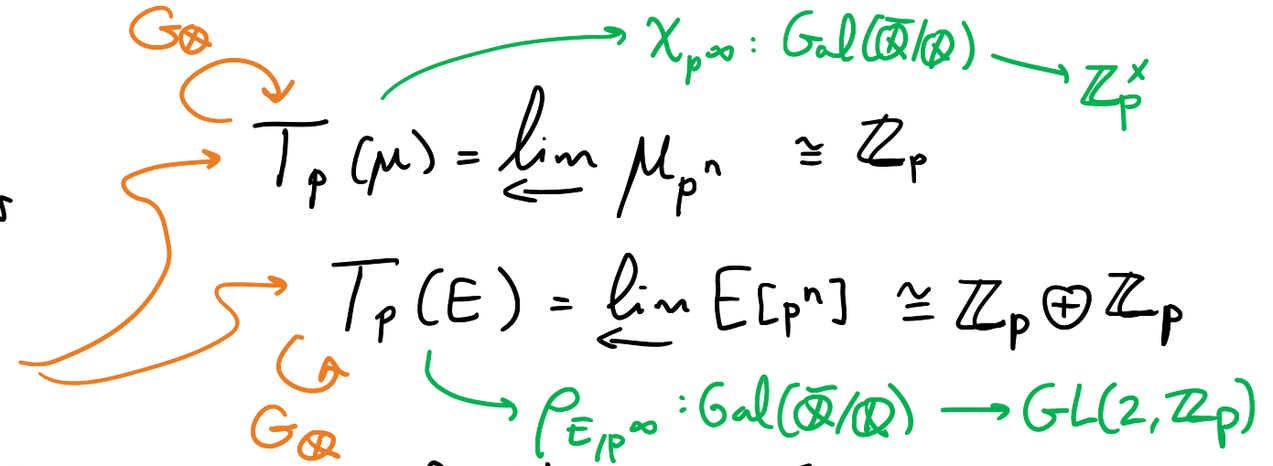
PREVIOUSLY...

- Weierstrass models
- Isogenies
- The Tate module



Theorem Let E/K be an elliptic curve, and let $m \geq 2$. There is a pairing

(The Weil pairing!) $e_m : E[m] \times E[m] \longrightarrow \mu_m$ $\left((S,T) \longmapsto e_m(S,T) = \frac{g_T(X+S)}{g_T(X)} \right)$

s.t. e_m is:

(a) Bilinear: $e_m(S_1+S_2, T) = e_m(S_1, T) \cdot e_m(S_2, T)$

$e_m(S, T_1+T_2) = e_m(S, T_1) \cdot e_m(S, T_2)$

(b) Alternating: $e_m(T,T) = 1$, $e_m(S,T) = e_m(T,S)^{-1}$.

(c) Non-degenerate: $e_m(S,T) = 1 \quad \forall S \in E[m] \Rightarrow T = 0$

(d) Galois-invariant: $\forall \sigma \in \mathrm{Gal}(\overline{K}/K) \quad e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$

(e) Compatible: if $S \in E[mm']$ and $T \in E[m]$, then

$e_{mm'}(S,T) = e_m([m']S, T)$

Corollary Let K be a field, let E/K be an ell. curve, and let $m \geq 2$. Define:

$$K(E[m]) = K\left(\{x(P), y(P)\} : P \in E[m]\right) \subseteq \overline{K}$$

the m-th "division field" or field of definition of $E[m]$.

(a) There are $S, T \in E[m]$ s.t. $e_m(S,T)$ is a primitive m-th root of unity.

(b) If $K(E[m]) \subseteq K$, then $\mu_m \subseteq K^*$. $\Rightarrow E(K) \supseteq E[m]$.

Proof.

(a) Consider $\{e_m(S,T) : S, T \in E[m]\} = \mu_d \subseteq \mu_m$ for some $d \mid m$. (μ_d is a subgroup of μ_m)

(In general, $K(E[m])/K$ is an extension of degree $\#GL(2, \mathbb{Z}/m\mathbb{Z})$)

$\Rightarrow 1 = e_m(S,T)^d = e_m([d]S, T)$ (bilinearity) Fix S, this is true $\forall T \in E[m]$.

$\Rightarrow [d]S = O \quad \forall S$ but if S is of exact order m then $\Rightarrow d = m$.

∎

(b) **If $K(E[m]) \subseteq K$ then $\mu_m \subseteq K^*$.**

$\forall \sigma \in G_{\bar{K}/K}$, $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) = e_m(S,T) = \zeta$

(σ: Gal inv; S^σ, T^σ: $E[m] \subseteq E(K)$)

then $\zeta^\sigma = \zeta$ for all $\sigma \in G_{\bar{K}/K}$ then $\sigma(S) = S$, $\sigma(T) = T$

If we pick S, T so that ζ = prim m-th of unity $\xrightarrow[\text{Gal. thy.}]{}$ $\zeta \in K^* \to \mu_m \subseteq K^*$. ▨

ex $\mu_m \subseteq \mathbb{Q} \Rightarrow m = 1$ or 2. Let $E/\mathbb{Q}$ be an elliptic curve.

so if $E[m] \subseteq E(\mathbb{Q})$ then $m = 1$ or 2.

ex $y^2 = x^3 - x$, $E[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} \subseteq E(\mathbb{Q})$.

ex If $E[4] \subseteq E(K)$, then $\mathbb{Q}(i) \subseteq K$. ($E[4]$: a # field.)

ex $E/\mathbb{Q}(i)$: $y^2 + xy + y = x^3 + x^2 - 10x - 10$

$E[4] = \langle (-2,-2), (-7, 3-15i) \rangle$

($(-2,-2) \in E(\mathbb{Q})$)

Prop. 8.2 Let $S \in E_1[m]$, $T \in E_2[m]$, and $\phi : E_1 \to E_2$ an isog. ($\hat{\phi}$)

Then, $e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$

(i.e., $\phi, \hat{\phi}$ are dual (adjoint) wrt. the Weil pairing).

- **Weil pairing on the Tate module:** $T_p(E) = \varprojlim E[p^n]$

$$e_{p^n} : E[p^n] \times E[p^n] \longrightarrow \mu_{p^n}$$

and $e_{p^{n+1}}(S,T)^p = e_{p^{n+1}}(S, [p]T)$ (bilinearity)

$= e_{p^n}([p]S, [p]T)$ (compatible)

$$\begin{array}{ccc} E[p^{n+1}] \times E[p^n] & \xrightarrow{e_{p^{n+1}}} & \mu_{p^{n+1}} \\ \downarrow [p] \quad \downarrow [p] & \circlearrowright & \downarrow \zeta \mapsto \zeta^p \\ E[p^n] \times E[p^n] & \xrightarrow{e_{p^n}} & \mu_{p^n} \end{array}$$

$\longrightarrow e : T_p(E) \times T_p(E) \longrightarrow T_p(\mu)$

is a bilinear, alternating, non-deg, Gal-inv

and $\phi, \hat{\phi}$ are adjoint for the pairing.

$e(S, \hat{\phi}(T)) = e(\phi(S), T)$

Corollary Let E/K be an ell. curve, let p be a prime. Let

$$\rho_{E,p^\infty} : \mathrm{Gal}(\bar{K}/K) \longrightarrow GL(2,\mathbb{Z}_p) \simeq \mathrm{Aut}(T_p(E))$$

$$\chi_{p^\infty} : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathbb{Z}_p^\times \simeq \mathrm{Aut}(T_p(\mu))$$

s.t. $\rho_{E,p^\infty}(\sigma)\left(P \mapsto \sigma(P)\right)$, s.t. $\chi_{p^\infty}(\sigma)\left(\zeta \longmapsto \zeta^\sigma\right)$.

Then, $\det(\rho_{E,p^\infty}) = \chi_{p^\infty}$.

Proof. Let $T_p(E) = \langle P, Q \rangle_{\mathbb{Z}_p}$, and $\rho_{E,p^\infty}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{Z}_p)$. (P Q)

Then,

$$e(P,Q)^\sigma = e(P,Q)^{\chi_{p^\infty}(\sigma)}$$

$$e(P^\sigma, Q^\sigma) = e([a]P + [c]Q, [b]P + [d]Q)$$

$$= e(P,P)^{ab} \cdot e(P,Q)^{ad} \cdot e(Q,P)^{bc} \cdot e(Q,Q)^{cd}$$

$$= e(P,Q)^{ad} \cdot e(P,Q)^{-bc} = e(P,Q)^{ad-bc}.$$

$\det(\rho_{E,p^\infty}(\sigma)) = \chi_{p^\infty}(\sigma)$ $\forall \sigma \in G_{\bar{K}/K}$

∎

$Q \in T_p(E)$

$Q = (Q_1, Q_2, Q_3, \dots, Q_n, \dots)$ s.t. $Q_i \in E[p^i]$

and $[p]Q_{n+1} = Q_n$.

$[a]Q = ([a]Q_1, [a]Q_2, \dots, [a]Q_n, \dots) \overset{?}{\in} T_p(E)$

$[p^n]([a]Q_n) = [a][p^n]Q_n = [a]O = O$

$\Rightarrow [a]Q_n \in E[p^n]$

and

$[p]([a]Q_{n+1}) = [a][p]Q_{n+1} = [a]Q_n.$

Elliptic Curves over Finite Fields

(Chapter V)

Let K be a finite field, with $q = p^n$ elements (p prime).

(e.g. $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $f(x) \in \mathbb{F}_p[x]$ irred. of degree n

$K = \mathbb{F}_p[x]/(f(x))$

ex $p=3$, x^2-2 irred over $\mathbb{F}_3$, $K = \mathbb{F}_3[x]/(x^2-2)$ is a field w/ q elts.)

E/K an elliptic curve, $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$ w/ $a_i \in K$

$\Delta \neq 0$ in K.

Q $\#E(K)$?

- $E(K) \subseteq (K \times K) \cup \{\mathcal{O}\}$

$\Rightarrow \#E(K) \leq q^2 + 1$.

For
- Each value of x there are at most 2 poss. values for y.

1 value if $\Delta = 0$
2 values if $\Delta \in (K^\times)^2$.

let Δ be the disc in y

FACT $\#(K^\times)^2 = \frac{q-1}{2}$

$\Rightarrow \#E(K) \leq 2q + 1$.

??? $\Rightarrow \#E(K) \simeq 2 \cdot \left(\frac{q-1}{2}\right) + 1 + 1 = q - 1 + 1 + 1 = q + 1$

Theorem (Conjectured by Artin, proved by Hasse in 1930's)

$$\left| \#E(k) - q - 1 \right| \leq 2\sqrt{q}.$$

Proof.

- Cor III.6.3. Let E_1, E_2 be ell. curves. Then the deg map:

$$\deg : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$$

is a positive definite quadratic form.

(quad form: $d : A \to \mathbb{R}$, $d(\alpha) = d(-\alpha)$; $A \times A \to \mathbb{R}$ is bilinear $(\alpha, \beta) \mapsto d(\alpha+\beta) - d(\alpha) - d(\beta)$

positive definite: $d(\alpha) \geq 0$, $d(\alpha) = 0 \Leftrightarrow \alpha = 0$)

- $\phi : E \longrightarrow E$

$(x, y) \longmapsto (x^q, y^q)$

Frobenius endomorphism ($q = p$ this is FLT.)

(note: coeffs of $E/k \Rightarrow a_i^q = a_i$)

$\deg \phi = q$

$$\phi : E \longrightarrow E$$
$$(x,y) \longmapsto (x^q, y^q)$$

- $E(K) = \ker(\mathrm{Id} - \phi)$ b/c $P \in E(K) \iff \phi(P) = P$.

$\#E(K) = \#\ker(\mathrm{Id}-\phi) = \deg(\mathrm{Id}-\phi)$.

$\phi(P) = \mathrm{Id}(P)$
$\Rightarrow (\mathrm{Id}-\phi)(P) = \mathcal{O}$.

So $\left|\#E(K) - 1 - q\right| = \left|\deg(\mathrm{Id}-\phi) - \deg(\mathrm{Id}) - \deg(\phi)\right| \leq 2\sqrt{1\cdot q} = 2\sqrt{q}$.

Lemma A an abelian gp., $d : A \to \mathbb{Z}$ is a pos. def. quad. form.
Then $\forall \psi, \phi \in A$: $\left|d(\psi-\phi) - d(\psi) - d(\phi)\right| \leq 2\sqrt{d(\phi)d(\psi)}$.

Pf. Let $L(\psi,\phi) = d(\psi-\phi) - d(\psi) - d(\phi)$ (bilinear b/c d quad. form)

Pos. def $0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mn\, L(\psi,\phi) + n^2 d(\phi)$.

Take $m = -L(\psi,\phi)$, $n = 2d(\psi)$

$\Rightarrow \quad 0 \leq \underbrace{d(\psi)}_{>0} \cdot \underbrace{\left(4d(\psi)d(\phi) - L(\psi,\phi)^2\right)}_{>0}$, $\psi \neq 0$

$\Rightarrow |L(\psi,\phi)| \leq \sqrt{4d(\psi)d(\phi)}$. ▨