Contents

$$t = q + 1 - \#E(\mathbb{F}_q)$$

So the characteristic polynomial of frobenius polynomial is $x^2 - tx + q$.

$$\Phi_q^2 - [t]\Phi_q + [q] = 0$$

Let α be that endomorphism so $\alpha \in \text{End(E)}$.

If $\alpha \neq 0$ then $\# \ker \alpha \leq \deg \alpha$, so $\ker \alpha$ is finite.

We now show that if $\alpha \neq 0$ then $\# \ker \alpha = \infty$.

For any int n such that $p \nmid n$,

$$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$$

and we represent

$$\Phi_q|_{E[n]} : E[n] \to E[n]$$

since it's an endomorphism that is just restricted to $E[n]$ so we can represent this as a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

So by direct inspection

$$A_n^2 - \text{tr}(A_n) \cdot A_n + \det(A_n) I = 0$$

We've shown that

$$\det(A_n) = \deg \Phi_q \mod n$$

Another calc shows

$$\text{tr}(A_n) = 1 + \det(A_n) - \det(I - A_n)$$

so

$$\text{tr}(A_n) = 1 + q - \deg(\text{id} - \Phi_q) \mod n$$

since $\deg(\text{id} - \Phi_q) = \#E(\mathbb{F}_q) = q + 1 - t$ so

$$A_n^2 - [1 + q - (q + 1 - t)]A_n + qI = 0$$

for 2x2 matrices. Remember that A_n is a matrix in $E[n]$ so the matrix is defined over mod n.

$$\underbrace{A_n^2 - [t]A_n + qI = 0}_{\text{representation of } \alpha|_{E[n]}}$$

This means that for any n such that $p \nmid n$ then for all $P \in E[n]$

$$\alpha(P) = 0$$

since the set

$$U_{p\nmid n}E[n]$$

is infinite (the U means union here),

$$\#\ker(\alpha) = \infty$$

contradiction.

Note: $t = \mathrm{tr}(A_n)\ \forall p \nmid n$ so is called the trace of Frobenius.

1 $\deg(\alpha \circ \alpha^{'}) = \deg(\alpha) \circ \deg(\alpha^{'})$

$$E \to E' \to E''$$

by the maps α', α.

For simplicity think $E = E' = E''$.

$$\alpha(x, y) = (R(x), yS(x))$$
$$\alpha'(x, y) = (R'(x), yS'(x))$$

Then $(\alpha \circ \alpha')(x, y)$ has repr:

$$(R''(x), yS''(x)) = (R(R'(x)), S(R'(x))S'(x)y)$$

So this already satisfies the property of canonical form. The other property is that both sides don't share a common root over the algebraic closure.

If $R(R'(x)) = \frac{u''(x)}{v''(x)}$ is a reduced rational function, then

$$\deg(\alpha \circ \alpha') = \max\{\deg u'', \deg v''\}$$

Reduced means no common roots over $\bar{K}$.

How do we prove $R(R'(x))$ is reduced? Lets write over $\bar{K}$

$$R(x) = \frac{\prod(x - \alpha_i)}{\prod(x - \beta_j)}$$

$$R'(x) = \frac{\prod(x - \alpha'_i)}{\prod(x - \beta'_j)}$$

$$R(R'(x)) = \frac{\prod(\frac{\prod(x-\alpha'_i)}{\prod(x-\beta'_j)} - \alpha_i)}{\prod(\frac{\prod(x-\alpha'_i)}{\prod(x-\beta'_j)} - \beta_j)}$$

if x_0 is such that

$$R'(x_0) = \alpha_i$$

for some i.

Then clearly since $a_i \neq \beta_j$ for all j.

$$R'(x_0) \neq \beta_j$$

Finally, a direct calculation shows that if

$$R''(x) = R(R'(x)) = \frac{u''(x)}{v''(x)}$$

then

$$\max\{\deg u'', \deg v''\} = \max\{\deg u, \deg v\} \max\{\deg u', \deg v'\}$$

$$R = u/v, R'' = u'/v'$$

$$R(R') = \frac{u(u'/v')}{v(u'/v')}$$

as rational functions,

$$\deg u(u'/v') = \deg u \max \{\deg u', \deg v'\}$$
$$\deg v(u'/v') = \deg v \max \{\deg u', \deg v'\}$$

(remember we are doing composition not multiplication)

$$R(R'(x)) = \frac{u''(x)}{v''(x)}$$

and

$$\begin{aligned}\max\{\deg u'', \deg v''\} &= \max\{u \max\{\deg u', \deg v'\}, v \max\{\deg u', \deg v'\}\} \\ &= \max\{u, v\} \max\{u', v'\} \\ &= \deg \alpha \deg \alpha'\end{aligned}$$

2 Isomorphic Isogeny

Isogeny $\alpha : E \to E'$ is called an isomorphism if $\exists$ an isogeny $\bar{\alpha}' : E' \to E$ such that $\alpha \circ \alpha^{-1} = \mathrm{id}_E$ and $\alpha^{-1} \circ \alpha = \mathrm{id}_E$.

2.1 $\deg \alpha = 1$ when α is an isomorphism

$$\deg \alpha \circ \deg \alpha^{-1} = \deg(\alpha \circ \alpha^{-1}) = \deg(\mathrm{id}_E) = 1$$
$$\Rightarrow \deg \alpha = 1$$

Remember E and E' might not be isomorphic over K but they might be isomorphic over an extension of K.

3 j-invariant

EC should be non-singular means $\Delta = 4A^3 + 27B^2 \neq 0$.

$$j = 1728 \frac{4A^3}{\Delta}$$

determines E up to isomorphism over $\bar{K}$.

A twist is you have two curves where $K \subseteq K'$

$$E(K), \quad E'(K')$$
$$E(K') \cong E'(K')$$

It also turns out $[K' : K]$ is only 2, 4 or 6 (quadratic, quartic, sextic twists).

For $E(K)$, you can calculate $\#\mathrm{Aut}_{\bar{K}}(E) \leq 24$.

Remark: if $A = 0$ then $j = 0$. If $B = 0$, then $j = 1728$.

3.1 Proof of j invariant

If $j = 0$ or 1728, then take $E : y^2 = x^3 + 1$ or $E : y^2 = x^3 + x$, otherwise

$$A = 3j_0(1728 - j_0), \; B = 2j_0(1728 - j_0)^2$$

Then we see the j-invariants are consistent.

3.2 We cannot use rational maps, only polynomials for isogenies

All well defined rational maps which map $R(x)$ or $S(x)$ to ∞ must map to (∞, ∞). To observe this just look at $y^2 = x^3 + Ax + B$.

Let $R(x) = \frac{p(x)}{q(x)}$, then there's a root of $q(x)$ which is x_0. Then $R(x_0) = \infty$, but $\alpha(\infty) = \infty$ so we have a contradiction.

3.3 Showing $A' = \mu^4 A, B' = \mu^6 B$

Since deg $\alpha = 1$, $R(x) = ax + b$ by the definition of degree for a rational map.

$$S^2(x)(x^3 + Ax + B) = (ax+b)^3 + A'(ax+b) + B'$$

so comparing coefficients, we see $c^2 = a^3$ so $\mu = c/a \in K^\times$ so $a = \mu^2$.

$$\mu^6(x^3 + Ax + B) = \mu^6 x^3 + A'\mu^2 x + B'$$

$$\Rightarrow A' = \mu^4 A, B' = \mu^6 B$$

3.4 Converse

Let $A' = \mu^4 A, B' = \mu^6 B$, $\alpha(x, y) = (\mu^2 x, \mu^3 y)$. Then α is a rational map that preserves ∞, so α is an isogeny. Also α has an inverse $\alpha^{-1}(x, y) = (x/\mu^2, y/\mu^3)$.

And then composing them clearly gives the identity.

4 Tate Pairing Recap

$$q = p^n, r | \#E(\mathbb{F}_q)$$

with r prime.

$$E[r] = \{P \in E(\bar{\mathbb{F}}_{q^k}) : rP = \infty\}$$

$$E[r] \subseteq E(\mathbb{F}_{q^k})$$

$$\tau : E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r$$

so this k is the embedding degree.

4.1 Embedding Degree

1. $r | \#E(\mathbb{F}_q)$
2. $\gcd(r, q-1)$

Embedding degree of E wrt r is the minimal k such that

$$r | q^k - 1$$

Also we assume $\gcd(r, k) = 1$.

We want to extract a type II bilinear pairing

$$G_1 \times G_2 \to G_T$$

$$|G_1| = |G_2| = |G_T| = r$$

For G_1, recall that $E(\mathbb{F}_q)$ has the property that for any $r | \#E(\mathbb{F}_q)$ there is a subgroup of order r with $|G_1| = r$.

Now we find the k such that we have G_2.

5 Balasubramanian-Koblitz

Theorem: $r | \#E(\mathbb{F}_q)$ and $\gcd(r, q-1) = 1$ then $E[r] \subseteq E(\mathbb{F}_{q^k})$ iff $r | q^k - 1$.

5.1 $r|q^k - 1 \Rightarrow E[r] \subseteq E(\mathbb{F}_{q^k})$

Hasse-Weil states that in $\mathrm{End}(E)$ then $\Phi^2 - [t]\Phi + [q] = 0$ where $t = q + 1 - \#E(\mathbb{F}_q)$.

Lemma: for r as above

$$(\Phi - [1])(\Phi - [q]) \equiv 0 \mod r$$

Denote $\#E(\mathbb{F}_q) = hr$. We usually call h the cofactor, and $p(x) = x^2 - tx + q$.

$$\begin{aligned} p(x) &= x^2 - tx + q \\ &= x^2 - (q + 1 - hr)x + q \\ &\equiv x^2 - (q+1)x + q \mod r \\ &\equiv (x-1)(x-q) \mod r \end{aligned}$$

Def: the lth eigenspace of Φ is

$$\mathrm{Eig}_\ell(\Phi) = \{P \in E(\bar{\mathbb{F}}_q) : \Phi(P) = \ell P\}$$

so for example the 1th eigenspace is simply $E(\bar{\mathbb{F}}_q)$.

We set $H_1 = \mathrm{Eig}_1(\Phi) \cap E[r]$ and $H_q = \mathrm{Eig}_q(\Phi) \cap E[r]$.

Corollary:

$$\begin{aligned} E[r] &= \{aP + bQ : P \in H_1, Q \in H_q\} \\ &= H_1 \times H_q \end{aligned}$$

(remembering E[r] contains points from the closure)

$$E[r] \subseteq \{R \in E(\bar{\mathbb{F}}_q) : (\Phi - 1)(\Phi - q)(R) = 0\}$$

$H_1 =$ roots of $\Phi - 1 \cap E[r]$, $H_q =$ roots of $\Phi - q \cap E[r]$.

5.2 Selecting G_1

r is prime and $E[r] \cong H_1 \times H_r$, so in practice a natural choice of G_1 is

$$G_1 = H_1 = E(\mathbb{F}_q)[r]$$

Def: let r be prime $r|\#E(\mathbb{F}_q)$ and $\gcd(r, q-1) = 1$ and k the embedding degree (minimal integer such that $r|q^k - 1$ and $\gcd(k, r) = 1$).

The trace map is

$$Tr : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q)$$

$$Tr(P) = P + \Phi(P) + \Phi^2(P) + \cdots + \Phi^{k-1}(P)$$

(not to be confused with trace of Frobenius)

Note Φ^k is the q^k-Frobenius map hence the identity.

$$\Phi : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q)$$

$$\Phi : E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$\Phi^k : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q)$$

$$\Phi^k : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$$

where 2nd and 4th lines are the identity.

$$\begin{aligned} \Phi(Tr(P)) &= \Phi(P + \Phi(P) + \Phi^2(P) + \cdots + \Phi^{k-1}(P)) \\ &= \Phi(P) + \Phi^2(P) + \Phi^3(P) + \cdots + \Phi^{k-1}(P) + P \\ &= Tr(P) \end{aligned}$$

so the trace image is fixed under action by Φ and hence

$$\mathrm{Im}(Tr) \subseteq E(\mathbb{F}_q)$$

and not only in $E(\mathbb{F}_{q^k})$.

Lemma: the k-eigenspace of Tr is $E(\mathbb{F}_q)[r] = H_1$.

If $R \in E(\mathbb{F}_q)[r]$ then $\Phi(R) = R$ which means $Tr(R) = R + ... + R = kR$. So R is a k eigenvector of the trace.

Likewise if $R \in E(\mathbb{F}_{q^k})$ such that $Tr(R) = kR$ then $\Phi(Tr(R)) = \Phi(kR) = k\Phi(R)$, and since $\Phi(Tr(R)) = Tr(R)$ then $\Phi(Tr(R)) = Tr(R)$. Then $k(\Phi(R) - R) = \infty \Rightarrow \Phi(R) = R$ since $\gcd(k, r) = 1$ since then $kP = \infty$ otherwise.

So Φ fixes all points $R \in E[r]$ such that $Tr(R) = kR$ hence such points must be in $E(\mathbb{F}_q)[r]$.

5.3 Defining G_2

1. $H_1 = E(\mathbb{F}_q)[r]$
2. $H_q = \{R \in E[r] : Tr(R) = \infty\}$

We see (1) is immediate from before.

Let $R \in E[r]$ with $Tr(R) = \infty$. Write $R = aP + bQ$ for $P \in H_1, Q \in H_q$.

$$\begin{aligned}\Phi(R) &= \Phi(aP + bQ)\\ &= aP + bqQ\\ \Phi^2(R) &= aP + bq^2Q\end{aligned}$$

$$\infty = Tr(R) = kaP + b(1 + q + \cdots + q^{k-1})Q$$

note that $1 + q + \cdots + q^{k-1} = \frac{q^k-1}{q-1}$.

$$\Rightarrow \infty = kaP + b\left(\frac{q^k - 1}{q - 1}\right)Q$$

so $a \equiv 0 \mod r$ since H_1, H_q are subgroups with trivial intersections.

Conversely, if $R = Q \in H_q$ then

$$Tr(Q) = \frac{q^k - 1}{q - 1}Q$$

but $r | q^k - 1$ and $r \nmid q - 1$ so $r | \frac{q^k-1}{q-1}$

$$\Rightarrow Tr(Q) = 0$$

5.4 <= of BR theorem

For E, r, k, q as above

$$E[r] \subseteq E(\mathbb{F}_{q^k})$$

Let $R \in E[r]$, write $R = aP + bQ$ with $P \in H_1, Q \in H_q$, then $Tr(Q) = \infty$ and

$$\Phi^k(Q) = q^kQ = Q$$

since $r | q^k - 1$. Furthermore

$$\Phi^k(P) = P$$

because $P \in E(\mathbb{F}_q)[r] \subseteq E(\mathbb{F}_q)$. Thus

$$\begin{aligned}\Phi^k(R) &= \Phi^k(aP + bQ)\\ &= aP + bQ\end{aligned}$$

so $E[r]$ is fixed by Φ^k hence

$$E[r] \subseteq E(\mathbb{F}_{q^k})$$