Contents

1 $\deg(\alpha \circ \alpha') = \deg(\alpha) \circ \deg(\alpha')$ **2**

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

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 $\alpha \in \mathrm{End(E)}$.

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

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

We've shown that

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

Another calc shows

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

so

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

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

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

(remember we are doing composition not multiplication)

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

and

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