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

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

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