Contents

Constructing the Algebraic Closure

Let p be prime and

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \cdots \subseteq \mathbb{F}_{p^n} \subseteq \cdots \subseteq \bar{\mathbb{F}}_p$$

$$\bar{\mathbb{F}}_p = \bigcup \mathbb{F}_{p^n}$$

Find a prime poly $f(x) \in \mathbb{F}_p[x]$ (i.e cannot be non-trivially factored such that deg $(f) = n$)

$$\mathbb{F}_p \subseteq \{\mathbb{F}_p[x] \bmod f(x)\} \subseteq \mathbb{F}_p$$

Balasubramanian-Koblitz Theorem

n is prime st. $n \mid \#E(\mathbb{F}_p)$ and $\gcd(n, p-1) = 1$. Then

$$E[n] \subseteq E(\mathbb{F}_{p^k}) \iff n \mid p^k - 1$$

The embedding degree of (E, n) is the minimal k st. $n \mid p^k - 1$.

Corollary

k is embedding degree of E, then $\mu_n \subseteq \mathbb{F}_{p^k}$.

Reduced Tate

$$\tau_n(P, Q) = f_{nD_P}(D_Q)^{\frac{p^k-1}{n}}$$

Equivalent Tate Pairing

Let Q_0 be such that $nQ_0 = Q$. Such a point is guaranteed to exist by the surjectivity of multiplication by n map.

$$\begin{tikzcd}
Q_0 \arrow[r] \arrow[d] & E(\mathbb{F}_{p^k}) \ni Q \arrow[d] \\
n : E(\overline{\mathbb{F}_{p^k}}) \arrow[r] & E(\overline{\mathbb{F}_{p^k}})
\end{tikzcd}$$

Then let $Q_1 = (\Phi^k - 1)(Q_0)$ where $Q_0 \in E[n]$ and Φ is the frobenius automorphism. Then $Q_1 \in E[n]$.

$$
\begin{aligned}
e_n(P, Q_1) &= \frac{g_P(S+Q_1)}{g_P(S)} \\
&= \tau_n(P, Q)
\end{aligned}
$$

Frobenius Fixed Points

$$\Phi : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$$

Abuse of notation:

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

$$\text{FixedPoints}(\Phi) = E(\mathbb{F}_p)$$

$$\Phi^k : \overline{\mathbb{F}_{p^k}} \to \overline{\mathbb{F}_{p^k}}$$

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

$$\text{FixedPoints}(\Phi^k) = E(\mathbb{F}_{p^k})$$

Tate Trick

$$\frac{\phi^k - 1}{n} : E(\mathbb{F}_{p^k}) \to E[n]$$

but $Q \in E(\mathbb{F}_{p^k})$

$$Q = nQ_0 \to (\Phi^k - 1)(Q_0) = Q_1$$

$$Q_0 \in E(\overline{\mathbb{F}_{p^k}})$$

Kernel of Map

$$\ker\left(\frac{\Phi^k - 1}{n}\right) = nE(\mathbb{F}_{p^k}) \subseteq E(\mathbb{F}_{p^k})$$

if $Q = nP \in E(\mathbb{F}_{p^k})$

$$
\begin{aligned}
\left(\frac{\Phi^k - 1}{n}\right)(nP) &= (\Phi^k - 1)(P) \\
&= \Phi^k P - P
\end{aligned}
$$

Restatement of Equivalency

$$\forall P \in E[n] \subseteq E(\mathbb{F}_{p^k})$$

$$\forall Q \in E(\mathbb{F}_{p^k})$$

$$Q_1 = \left(\frac{\Phi^k - 1}{n}\right)(Q)$$

$$\implies \tau_n(P, Q) = e_n(P, Q_1)$$

By 1st isomorphism theorem

$$\frac{\Phi^k - 1}{n} : E(\mathbb{F}_{p^k}) \to E[n]$$

$$E(\mathbb{F}_{p^k}) / nE(\mathbb{F}_{p^k}) \cong \text{Im}\left(\frac{\Phi^k - 1}{n}\right)$$