④ Given: $E/\mathbb{F}_q$ - elliptic curve

ℓ - prime s.t. $\ell \nmid q$

k. s.t. $E[\ell] \subset E(\mathbb{F}_{q^k})$

$P, Q \in E(\mathbb{F}_q)$

I) Prove: If P, Q form a basis $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, then $e_\ell(P,Q)$ is a primitive ℓ-th root of unity in $\mathbb{F}_{q^k}$

Proof: Suppose $e_\ell(P,Q)$ was not primitive. Then, there must exist some $n < \ell$ for which $e_\ell(P,Q)^n = 1$. We also know that

$$\text{i) } e_\ell(P,Q)^n = e_\ell([n]P, Q) = 1$$

from the bilinearity of the Weil pairing.

For any $T \in [\ell]$, we have $T = [a]P + [b]Q$, $a, b \in \mathbb{Z}$, so:

$$e_\ell([n]P, T) = e_\ell([n]P, P)^a \cdot e_\ell([n]P, Q)^b =$$

$$= e_\ell(P,P)^{an} \cdot e_\ell([n]P, Q)^b$$

From the alternating of the Weil pairing and i) we have that

$$e_\ell(P,P)^{an} \cdot e_\ell([n]P, Q)^b = 1^{an} \cdot 1^b = 1$$

By the non-degeneracy of the Weil pairing, we have $[n]P = 0$. But, we have defined P as part of a basis of $E[\ell]$, so $|P| = \ell$. We therefore arrive at a contradiction. ∎

□

II) $\frac{1}{\ell}$

⑥ From HW10, ⑥a) we know that if an elliptic curve $E/\mathbb{F}_p$ defined by $E: y^2 = f(x)$ with $f(x)$ being and odd function and $p \equiv 3 \mod 4$, we have $|E(\mathbb{F}_p)| = p+1$.

For the curve in question, we have an odd function $(y^2 = x^3 - x)$ and a prime which is $p \equiv 3 \mod 4$. So we ~~have~~ know $|E(\mathbb{F}_p)| = p+1$.

~~By Th. 13.B~~ : We have the Frobenius trace $a_p = p+1 - p+1 = 0$. By Th. 13.5, we have that the curve in question is supersingular, and, as we found out in class, supersingular are vulnerable to the MOV attack.