

Math 497A Homework 9
Fall 2008
Due: Friday, November 7

- (1) Let E be an elliptic curve defined over \mathbb{F}_q (with $q = p^r$), and assume that $E[p] \cong \mathbb{Z}/p\mathbb{Z}$. Show that the Frobenius endomorphism ϕ_q is not multiplication-by- m for any integer m .
- (2) Let E be an elliptic curve defined over a finite field \mathbb{F}_q and suppose that

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$$

for some integer n . Show that either $q = n^2 + 1$ or that $q = n^2 \pm n + 1$ or $q = (n \pm 1)^2$.

(Hint: First show that $a = q + 1 - \deg(\phi_q - 1)$ is congruent to 2 modulo n .)

- (3) Let E be an elliptic curve defined over a finite field \mathbb{F}_q . Let $P, Q \in E(\mathbb{F}_q)$. Let N be the order of P . Assume that $\gcd(N, q) = 1$. Prove that there exists a k such that $Q = kP$ if and only if $NQ = \mathcal{O}$ and the Weil pairing $e_N(P, Q) = 1$.
- (4) Let E be an elliptic curve defined over \mathbb{F}_q . Give a direct proof of the fact that the Frobenius $\phi_q : E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_q)$ is surjective.
- (5) Let E be an elliptic curve defined over \mathbb{F}_q (with $q = p^r$), and ϕ_q the q -th power Frobenius. We say that E is *supersingular* if $\text{trace}(\phi_q) \equiv 0 \pmod{p}$.
- (a) Is it possible that ϕ_q is multiplication-by- m for some integer m ?
 - (b) Suppose now that $q = p$ is a prime > 3 . Prove that E is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$.
 - (c) What can you say about the p -torsion on a supersingular elliptic curve which is defined over a finite field of characteristic p ? (Try some examples of supersingular curves.)
- (6) Suppose Alice, Bob, and Chris want to share a secret. They can only meet in public, and they want to use an elliptic curve to set up a common shared secret that only the three of them know, even though everybody can listen in to all of their conversations. Explain how this can be done.