Edoardo Persichetti Lecture 7: Elliptic Curves 02/04/2014

Exercise 1 Let $s_n = \alpha^n + \beta^n$ be a sequence. Show that this is equivalent to the recurrence relation $s_{n+1} = as_n - qs_{n-1}$ with initial conditions $s_0 = 2, s_1 = a$.

Definition 1 (Roots of Unity) We define with μ_n the group of n-th roots of unity in a field $\mathbb{K}$, i.e. $\mu_n = \{x \in \bar{\mathbb{K}} \mid x^n = 1_{\mathbb{K}}\}$.

Lemma 1 *Let E be an elliptic curve defined over a field $\mathbb{K}$, $n \in \mathbb{Z}^+$. Then $E[n] \subset E(\mathbb{K}) \Rightarrow \mu_n \subset \mathbb{K}$.*

Lemma 2 *Let $q = p^k$ and $n \in \mathbb{Z}^+$ such that $p \not| n$. Then $\mu_n \subseteq \mathbb{F}_q^* \Leftrightarrow n|q-1$.*

Exercise 2 Let E be an elliptic curve defined over $\mathbb{F}_q$. Prove that, if $E(\mathbb{F}_q) \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$ for some n, then either $q = n^2 + 1$ or $q = n^2 \pm n + 1$ or $q = (n \pm 1)^2$.

Hint: use previous lemmas.

Exercise 3 Let $q \geq 5$ be a prime, and let E be an elliptic curve defined over $\mathbb{F}_q$. Prove that E is super singular if and only if $a = 0$. Not that this is equivalent to $\#E(\mathbb{F}_q) = q + 1$.

Exercise 4 Let E be an elliptic curve defined over $\mathbb{F}_q$ and suppose $a = q + 1 - \#E(\mathbb{F}_q) = 0$. Let $n \in \mathbb{Z}^+$. Show that if there exists a point of order n on the curve, then $E[n] \subseteq E(\mathbb{F}_{q^2})$ (in other words, the embedding degree is 2 in this case).

Exercise 5 Let $E : y^2 = x^3 - 20x + 21$ be defined over $\mathbb{F}_{35}$, and let $P = (15, -4)$. Show that it is possible to use Lenstra's factorization algorithm to factor 35 in two different ways.