MATH-GA 2150.001: Homework 4

1. Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Show that the group $E(\mathbb{F}_q)$ is either a cyclic group $\mathbb{Z}/n$ for some $n \geq 1$, or the group $\mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$ with $n \geq 1$ and $n_1, n_2 \geq 1$ integers, $n_1 \,|\, n_2$.

2. Let E be an elliptic curve defined over an algebraically closed field k, $char.k \neq 2, 3$. Recall that $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$ for any n prime to $car\, k$. Let $\{T_1, T_2\}$ be a base of $E[n]$.

   (a) Let $\zeta = e_n(T_1, T_2)$ and let d be an integer such that $\zeta^d = 1$. Show that $e_n(T_1, dT_2) = 1$ and that $e_n(T_2, dT_2) = 1$. Deduce that for all $S \in E[n]$ one has $e_n(S, dT_2) = 1$.

   (b) Show that $e_n(T_1, T_2)$ is a primitive n^{th} root of unity.

3. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. Assume $E(\mathbb{F}_q) = \mathbb{Z}/n \oplus \mathbb{Z}/n$.

   (a) Show that $(n, p) = 1$.

   (b) Show that $E(\overline{\mathbb{F}}_q)[n] \subset E(\mathbb{F}_q)$. Deduce that $\mu_n \subset \mathbb{F}_q$.

   (c) Let $a = q + 1 - \#E(\mathbb{F}_q)$. Deduce that $a \equiv 2 (\mathrm{mod}\, n)$.

   (d) Show that $q = n^2 + 1$ or $q = n^2 \pm n \pm 1$ or $q = (n \pm 1)^2$.