MATH-GA 2150.001: Homework 5

1. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$.

   (a) Show that a map α from $E(\mathbb{F}_p)$ to itself is injective if and only if it is surjective (α is not necessarily an endomorphism).

   (b) Show that if $E(\mathbb{F}_q)$ has no point of order n, then $E(\mathbb{F}_q)/nE(\mathbb{F}_q) = 0$.

2. Let $E : y^2 = x^3 + ax + b$ be an ellptic curve defined over a finite field $\mathbb{F}_p$, $E(\mathbb{F}_p) = \mathbb{Z}/m \oplus \mathbb{Z}/M$, $m|M$. For $d \in \mathbb{F}_p$ non square we define a *twist* of E as an elliptic curve E' given by the equation $y^2 = x^3 + ad^2x + bd^3$. Let $a = p+1-\#E(\mathbb{F}_p)$ and $a' = p+1-\#E'(\mathbb{F}_p)$. We also write $E'(\mathbb{F}_p) = \mathbb{Z}/n \oplus \mathbb{Z}/N$, where $n|N$.

   (a) Show that after a linear change of coordinates one can write E' as $dy^2 = x^3 + ax + b$. Deduce that $a = -a'$.

   (b) Show that $(m^2, n^2)|2a$.

   (c) Show that $a \equiv 2(\text{mod } m)$ and that $a \equiv -2(\text{mod } n)$ (one could use that $E(\overline{\mathbb{F}}_p)[m] \subset E(\mathbb{F}_p)$).

   (d) Deduce that $(m^2, n^2)|4$.

   (e) Show that the restriction of the Frobenius ϕ_p to $E'(\overline{\mathbb{F}}_p)[n^2]$ is given by a matrix
   $$\begin{pmatrix} 1+sn & tn \\ un & 1+vn \end{pmatrix}$$
   with $a \equiv 2 + (s+v)n \ (\text{mod } n^2)$ and
   $$p \equiv 1 + (s+v)n \ (\text{mod } n^2).$$
   Deduce that $4p \equiv a^2(\text{mod } n^2)$.

   (f) Show that $\frac{m^2n^2}{4} \leq 4p - a^2$.

   (g) Deduce that for p sufficiently big, either the curve E or the curve E' has a point of order bigger than $4\sqrt{p}$.