MATH-GA 2150.001: Homework 3

1. Show that the cubic curve $Y^2Z = X^3 + AXZ^2 + BZ^3$ is smooth iff $4A^3 + 27B^2 \neq 0$.

2. Let k be an algebraically closed field and let E be an elliptic curve over k defined by the equation $y^2 = x^3 + ax + b$. Write $f(x) = x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$. Show that the discriminant $\Delta = -(4a^3 + 27b^2)$ of E is given by the formula $\Delta = [(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)]^2$.

3. Let k be an algebraically closed field.
   (a) Let E be an elliptic curve over k given by the equation $y^2 = x^3 + Ax + B$. Show that $(x, y) \to (x, -y)$ is an endomorphism of E.
   (b) Let E be an elliptic curve over k given by the equation $y^2 = x^3 + B$. Show that $(x, y) \to (\zeta x, -y)$, where $\zeta^3 = 1$ is a primitive root of unity, is an endomorphism of E.
   (c) Let E be an elliptic curve over k given by the equation $y^2 = x^3 + Ax$. Show that $(x, y) \to (-x, iy)$ is an endomorphism of E.

4. **[j-invariant]** Let k be an algebraically closed field of characteristic different from 2 or 3. Let E be an elliptic curve given by an equation $y^2 = x^3 + Ax + B$. Define the j-invariant of E by the formula
$$j = j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}.$$
   (a) Let E_i be two elliptic curves given by the equations $y^2 = x^3 + A_i x + B_i$. Show that if $j(E_1) = j(E_2)$, then there exists $\mu \in K$, $\mu \neq 0$ such that $A_2 = \mu^4 A_1$ et $B_2 = \mu^6 B_1$.
   (b) Deduce that the map $x_2 = \mu^2 x_1$, $y_2 = \mu^3 y_1$ is a group isomorphism between E_1 and E_2.

5. (a) Let E be an elliptic curve over a field k (of characteristic different from 2) defined by the equation $y^2 = (x - e_1)(x - e_2)(x - e_3)$. Determine all the points of order 2 of E. Deduce the group structure on $E[2] = \{P \in E(k), 2P = 0\}$.
   (b) Let $a \in \mathbb{Z}$ be an integer not divisible by a 4^{th} power (but 1) and let E be the elliptic curve $y^2 = x^3 + ax$. The goal is to find all points of order 2^n of $E(\mathbb{Q})$.
      i. Determine all points of order 2.
      ii. Let $(x, y), (u, v) \in E$ with $(x, y) = 2(u, v)$. Show that $x = (u^2 - a)^2/4v^2$.
      iii. Let P be a point of order 2. Show that $P = 2Q$ implies $a = 4$. Find all points of order 4.
      iv. Conclude.