7. Let $y^2 = f(x)$ define an elliptic curve $E$ over $\mathbb{Q}$, where $f(x) \in \mathbb{Z}[x]$ is a cubic polynomial.

(a) If $E$ has good reduction at $p$, show that

$$|E(\mathbb{F}_p)| = 1 + p + \sum \left( \frac{f(x)}{p} \right)$$

where () is the Legendre symbol and the sum is over all $x \in \mathbb{F}_p$.

(b) Deduce that $E$ is supersingular (over $\mathbb{F}_p$) if and only if the coefficient of $x^{p-1}$ in $f(x)^{(p-1)/2}$ is zero. [Hint: calculate $\sum x^i$ over $x \in \mathbb{F}_p$.]

(c) Henceforth assume that $f(x) = x^3 + Dx$. Show that if $(p, 2D) = 1$, then $E$ has good reduction at $p$.

(d) Show that $E$ is supersingular (over $\mathbb{F}_p$) if $p \equiv 3 \pmod{4}$.

(e) Assuming that the torsion of $E(\mathbb{Q})$ injects into $E(\mathbb{F}_p)$ for $p \neq 2$, a prime of good reduction, calculate this torsion in terms of $D$.

(f) You should have found that $E(\mathbb{Q})$ always contains a nontrivial point $P$ of order 2. In such a situation there is always a unique elliptic curve $E'$ and a separable isogeny $\phi : E \to E'$ defined over $\mathbb{Q}$ such that ker($\phi$) = {O, P}, where O is the point at infinity on $E$.

Show that if $E'$ is given by $y^2 = x^3 - 4Dx$ and $\phi : E \to E'$ by

$$\phi(x, y) = (y^2/x^2, y(D - x^2)/x^2)$$

then this is such an isogeny. What is $\deg(\phi)$? [Remark: this isogeny is useful for calculating the rank of $E(\mathbb{Q})$.]