Math 497A Homework 10
Fall 2008
Due: Friday, November 14

(1) Let $E$ be an elliptic curve defined over $\mathbb{F}_q$, and suppose that $a = q + 1 - \#E(\mathbb{F}_q) = 0$. Let $N$ be a positive integer. Show that if there exists a point $P \in E(\mathbb{F}_q)$ of order $N$, then the full $N$-torsion is defined over $\mathbb{F}_q^2$, i.e. $E[N] \subseteq E(\mathbb{F}_q^2)$.

(2) Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. Let $\ell$ be a prime such that $\ell \mid \#E(\mathbb{F}_q)$, $E[\ell] \nsubseteq E(\mathbb{F}_q)$, and $\ell \nmid q(q-1)$. Show that

$E[\ell] \subseteq E(\mathbb{F}_{q^m})$ if and only if $q^m \equiv 1 \mod \ell$.

(Hint: One direction is easy. For the other direction, show that (for $\ell \nmid q$) you can choose a basis $\{P, Q\}$ for the $\ell$-torsion with $P \in E(\mathbb{F}_q)$, $Q \notin E(\mathbb{F}_q)$, and consider the action of $\phi_q$ and of $\phi_q^m$ on the $\ell$-torsion.)

(3) Let $E$ be the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$.
   (a) Show that $f(x, y) = (y^4 + 1)/(x^2 + 1)^3$ has no zeros or poles in $E(\mathbb{Q})$.
   (b) Show that $g(x, y) = y^4/(x^2 + 1)^3$ has no poles in $E(\mathbb{Q})$ but does have zeros in $E(\mathbb{Q})$.
   (c) Find the divisors of $f$ and $g$ (over $\overline{\mathbb{Q}}$).

(4) Let $E$ be the elliptic curve

$E : y^2 = x^3 + 4x$

defined over $\mathbb{F}_{11}$. Let

$D = [(0, 0)] + [(2, 4)] + [(4, 5)] + [(6, 3)] - 4[O]$.

(a) Show that $D$ is the divisor of a function on $E$. In the following parts we will find this function.

(b) Compute the equation for the line $\ell(x, y) = 0$ through the points $(0, 0)$ and $(2, 4)$. Compute the divisor of $\ell(x, y)$.

(c) Similarly, compute the divisor of $(x - 2)$ and of $(y + x + 2)$.

(d) Show that

$D = [(2, -4)] + \text{div} \left( \frac{\ell(x, y)}{x - 2} \right) + [(2, 4)] + \text{div} \left( \frac{y + x + 2}{x - 2} \right) - 2[O]$.

(e) Find a function $f(x, y)$ whose divisor is $D$. Use the fact that $x$ and $y$ satisfy the curve equation for $E$ to simplify your answer.

(5) Let $E$ be an elliptic curve defined over a field $K$, and let $m, n$ be positive integers that are not divisible by the characteristic of $K$. Let $S \in E[mn]$ and $T \in E[n]$. Show that

$e_{mn}(S, T) = e_n(mS, T)$. 