MATH 845: HOMEWORK 5, DUE APR 15.

9. Let E be an elliptic curve over $\mathbf{F}_q$.

(a) Show that $E(\mathbf{F}_q) \cong \mathbf{Z}/m \times \mathbf{Z}/mn$ for some integers $m, n \geq 1$ with $\gcd(m, q) = 1$.

(b) With the notation of (a), show that $q \equiv 1 \pmod{m}$.

(c) Suppose that q is a prime ≥ 5 and that E is supersingular. Show that $m = 1$ or 2. If $q \equiv 1 \pmod{4}$, prove that $m = 1$.

10. Let E be the elliptic curve $y^2 = x^3 + 16$.

(a) Show that this equation defines an elliptic curve over $\mathbf{F}_p$(p prime) if and only if $p \geq 5$.

(b) Calculate a_5 and a_7 where $a_p = p + 1 - |E(\mathbf{F}_p)|$.

(c) Which kind of singularity does the equation have over $\mathbf{F}_3$? What should we take a_3 to be (is the given equation minimal at 3)?

(d) For $p = 2$ we have to proceed differently since the equation is not in "minimal form" for $p = 2$. Give a $\mathbf{Q}$-linear change of variables taking the equation of E to $y^2 + y = x^3$. Does this curve have good reduction at $p = 2$? What is a_2?

(e) Calculate $L(E, s) = \sum_{n=1}^{\infty} c_n/n^s$ up to and including the $n = 10$ term.

(f) Let $\mathbf{Z}[\omega]$ ($\omega = e^{2\pi i/3}$) denote the ring $\{a + b\omega : a, b \in \mathbf{Z}\}$. Define the norm $N(a + b\omega) = a^2 - ab + b^2$. If $\gcd(Nx, 3) = 1$, let $\chi(x) = (-\omega)^j$ be the unique 6th root of 1 such that $x\chi(x) \equiv 1 \pmod{3}$. Let $\chi(x) = 0$ for all other x. Compute $\sum_{x \in \mathbf{Z}[\omega], \neq 0} \chi(x)x/(Nx)^s$ as a Dirichlet series up to $Nx \leq 10$ and hence conjecture an expression for $L(E, s)$.