MATH 844: HOMEWORK 3, DUE OCT 27.

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

(i) Let d be any positive integer. By representing $E[d]$ as the kernel of an isogeny, show that $|E[d]| \leq d^2$.

(ii) Show that $E(\mathbf{F}_q) \cong \mathbf{Z}/m \times \mathbf{Z}/mn$ for some positive integers m, n with $\gcd(m, q) = 1$. (You may quote previous homeworks.)

(iii) Look up what the Weil pairing is. Assuming its existence, show that $q \equiv 1 \pmod{m}$.

(iv) Either find an elliptic curve E over some prime field $\mathbf{F}_p$ with $E(\mathbf{F}_p) \cong \mathbf{Z}/11 \times \mathbf{Z}/11$ or else show that no such p and E exist.

2. Let E be the elliptic curve $y^2 + y = x^3 - x^2$ defined over $\mathbf{Q}$. Let $\rho_p : G_{\mathbf{Q}} \to GL_2(\mathbf{F}_p)$ denote the associated Galois action on $E[p]$.

(a) Find an equation for the x-coordinates of the points in $E[2]$. Find the image of ρ_2.

(b) Find an equation for the x-coordinates of the points in $E[3]$. Show that the only subgroup of $GL_2(\mathbf{F}_3)$ that surjects onto $PGL_2(\mathbf{F}_3)$ is $GL_2(\mathbf{F}_3)$. Find the image of ρ_3. Does E have complex multiplication?

(c) Find a point in $E(\mathbf{Q})$ of order 5. What does this tell us about the image of ρ_5?