MATH 844: HOMEWORK 5, DUE OCT 25.

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.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX