Additional exercises

MAT 1210, Univ. of Toronto, Spring 2015

Florian Herzig

1) Suppose $E/\mathbb{F}_q$, elliptic curve, $\ell \nmid q$ prime.
  (i) Show $\mathrm{End}\, E \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra (without using III.9!).
  (ii) Show $\mathbb{Q}[\varphi_q] \subset \mathrm{End}\, E \otimes_{\mathbb{Z}} \mathbb{Q}$ is a field.
  (iii) Deduce that $f(\varphi_q) = 0$ for some monic irred. poly. $f \in \mathbb{Q}[x]$.
  (iv) Show that φ_q acts semisimply on $V_\ell E := T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \approx \mathbb{Q}_\ell^2$
  (i.e. as a matrix over $\overline{\mathbb{Q}}_\ell$ it is diagonalizable).

2) (i) Suppose $E/\mathbb{F}_q$ is supersingular. Show that for some $n \geq 1$,
  $\mathrm{End}_{\mathbb{F}_{q^n}} E = \mathrm{End}\, E$ (an order in a quaternion algebra).
  (ii) Deduce that $\varphi_{q^n} \in \mathbb{Z}$ (hint: it lies in the centre), and hence that $\#E(\mathbb{F}_{q^{2n}}) = (q^n - 1)^2$.
  (iii) Deduce that any two supersingular elliptic curves over $\overline{\mathbb{F}}_p$ are isogenous.
  (iv) (Optional) Give another proof of Ex. 5.10(f) in Silverman.

3) Suppose E, E' are elliptic curves over K of char$(K) = p > 0$.
  (i) Suppose $\varphi : E \to E'$ is an isogeny of degree p. Show that (up to isomorphism) $\varphi = \varphi_p$ or $\varphi = \hat{\varphi}_p$.
  (ii) Show that these two possibilities coincide (up to isomorphism) iff E is supersingular.