Elliptic curves. Fall 2018

Assignment 4. Due Wednesday November 14.

Directions:

Undergraduate students answer 2 problems at their choice.
M.SC. students answer 3 problems at their choice.
Ph.D. students answer 4 problems at their choice.

1. Show directly that

$$\operatorname{rank}_{\mathbb{Z}} \operatorname{Hom}(E_1, E_2) \leq \operatorname{rank}_{\mathbb{Z}_\ell} \operatorname{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell.$$

2. (Silverman III.3.15) Let E_1/K and E_2/K be elliptic curves, and let $\phi : E_1 \to E_2$ be an isogeny of degree m defined over K where m is prime to $\operatorname{char}(K)$ if $\operatorname{char}(K) > 0$.

(a) Mimic the construction of the Weil pairing to construct a pairing

$$e_\phi : \ker(\phi) \times \ker(\hat{\phi}) \to \mu_m.$$

(b) Prove that e_ϕ is bilinear, nondegenerate and Galois invariant.

(c) Prove that e_ϕ is compatible in the sense that if $\psi : E_2 \to E_3$ is another isogeny, then

$$e_{\psi\circ\phi}(P, Q) = e_\psi(\phi P, Q)$$

for all $P \in \ker(\psi \circ \phi)$ and $Q \in \ker(\widehat{\psi})$.

3. (Silverman III.3.32) Let $\phi \in \operatorname{End}(E)$ be an endomorphism, and let $d = \deg \phi$ and $a = 1 + \deg \phi - \deg(1 - \phi)$.

(a) Prove that $\phi^2 - [a] \circ \phi + [d] = [0]$ in $\operatorname{End}(E)$.

(b) Let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $t^2 - at + d$. Prove that

$$|\alpha| = |\beta| = \sqrt{d}.$$

(c) Prove that $\deg(1 - \phi^n) = 1 + d^n - \alpha^n - \beta^n$ for all $n \geq 1$, and deduce that

$$|\deg(1 - \phi^n) - 1 - d^n| \leq 2d^{n/2}.$$

(d) Prove that

$$\exp\left(\sum_{n=1}^{\infty} \frac{\deg(1-\phi^n)}{n} X^n\right) = \frac{1 - aX + dX^2}{(1-X)(1-dX)},$$

and that the series converges for $|X| < |d|^{-1}$.

Hint: Use (III.8.6). For (b), use the fact that $\deg([m] + [n] \circ \phi) \geq 0$ for all $m, n \in \mathbb{Z}$.

4. (Silverman III.3.18)

5. (Silverman III.3.19)

6. (Silverman III.3.20)