Elliptic curves. Fall 2018

Assignment 3. Due Wednesday October 24.

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. Prove the following form of the Riemann-Roch theorem for $\mathbb{P}^1$:
Let $D \in \mathrm{Div}(C)$, $\deg(D) \geq 0$. Then, $\ell(D) = \deg(D) + 1$.

2. Use the Riemann-Hurwitz formula to find the genus of the following smooth plane curves, defined over a field K of characteristic zero.

(a) Show that the genus of the Fermat curves $x^n + y^n = 1$ is $(n-1)(n-2)/2$.

(b) Show that the genus of the hyperelliptic curves $y^2 = f(x)$, where $f(x)$ is a polynomial in $K[x]$ of degree d with distinct roots is $\lfloor (d-1)/2 \rfloor$.

3. (Silverman III.3.5) Let E/K be given by a singular Weierstrass equation.

(a) Suppose that E has a node, and let the tangent lines at the node be

$$y = \alpha_1 x + \beta_1, \quad \text{and} \quad y = \alpha_2 x + \beta_2.$$

If $\alpha_1 \in K$, show that $\alpha_2 \in K$ and $E_{\mathrm{ns}}(K) \simeq K^*$. If $\alpha_1 \notin K$, prove that $L = K(\alpha_1, \alpha_2)$ is a quadratic extension of K. Note that we know by the above that $E_{\mathrm{ns}}(K) \subseteq E_{\mathrm{ns}}(L) \simeq L^*$. Prove that

$$E_{\mathrm{ns}}(K) = \left\{ t \in L^* \ : \ N_{L/K}(t) = 1 \right\}.$$

(b) Suppose that E has a cusp. Prove that $E_{\mathrm{ns}}(K) \simeq K^+$.

(c) Let $p > 3$ be a prime, and let $K = \mathbb{F}_p$. Show that

$$\#E_{\mathrm{ns}}(\mathbb{F}_p) = \begin{cases} p & \text{if } E \text{ has a cusp;} \\ p-1 & \text{if } E \text{ has a node and the tangent lines are defined over } \mathbb{F}_p; \\ p+1 & \text{if } E \text{ has a node and the tangent lines are not defined over } \mathbb{F}_p. \end{cases}$$

4. Let $E/\mathbb{C}$ be an elliptic curve. Then there is a lattice Λ_E such that $E(\mathbb{C})$ is isomorphic to the abelian group $\mathbb{C}/\Lambda_E$ (see Silverman VI.5.1.1). Assuming this result, prove that

$$\deg[m] = m^2 \quad \text{and} \quad E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

5. (Silverman III.3.9) Let K be a field with $\mathrm{char}(K) \neq 2, 3$, and let E/K be an elliptic curve given by an homogeneous Weierstrass equation

$$F(X_0, X_1, X_2) = X_1^2 X_2 - X_0^3 - A X_0 X_2^2 - B X_2^3 = 0,$$

i.e. $x = X_0/X_2$ and $y = X_1/X_2$ are the Weierstrass coordinates. Let $P \in E$.

(a) Show that $[3]P = \mathcal{O}$ if and only if the tangent line to E at P intersect E only at P.

(b) Show that $[3]P = \mathcal{O}$ if and only if the Hessian matrix

$$\left(\frac{\partial^2 F}{\partial X_i \partial X_j}(P) \right)_{0 \leq i,j \leq 2}$$

has determinant 0.

(c) Show that $E[3]$ consists of 9 points.

6. (Silverman III.3.6)

7. (Silverman III.3.7) You can do only part of it, as there is (a)-(g), and this is very long.