Elliptic curves. Fall 2018

Partial Solutions to 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, $\ell(D) = \deg(D) + 1$.

Solutions: We first recall that if $D \sim D'$, then $\mathcal{L(D)} \simeq \mathcal{L(D')}$ and so $\ell(D) = \ell(D')$. Let D be any divisor of degree $n \geq 0$ on $\mathbb{P}^1$. Then, $D' = D - n([0,1])$ has degree 0, and since on $\mathbb{P}^1$ every divisor of degree 0 is principal, we have that $D \sim n([0,1])$, and it suffices to prove the result for $D_n = n([0,1])$, $n \geq 0$. We claim that

$$\left\{ 1, \frac{Y}{X}, \dots, \frac{Y^n}{X^n} \right\}$$

is a basis for $\mathcal{L}(D_n)$. First, we have that 1 and $\frac{Y^k}{X^k} \in \mathcal{L}(D_n)$ for all $1 \leq k \leq n$ since

$$\mathrm{div}\left(\frac{Y^k}{X^k}\right) = k(\mathcal{O}) - k([0,1]).$$

Now recall that any function $f \in \overline{K}(\mathbb{P}^1)$ is a quotient of 2 homogenous polynomials of the same degree. Then, any function $f \in \mathcal{L}(D_n)$ can be written as

$$f = \frac{a_k X^k + a_{k-1} X^{k-1} Y + \cdots + a_0 Y^k}{X^k},$$

since $f \in \mathcal{L}(D_n)$ only has poles at $[0,1]$. But then

$$f = a_k + a_{k-1} \frac{Y}{X} + \cdots + a_0 \frac{Y^K}{X^k},$$

and this proves that

$$\mathcal{L}(D_n) = \overline{K} \oplus \overline{K} \frac{Y}{X} \oplus \cdots \oplus \overline{K} \frac{Y^n}{X^n},$$

and so $\ell(D_n) = n + 1$ as claimed.

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 $\lfloor (d-1)/2 \rfloor$.

Solutions: (a) Let $F : x^n + y^n = 1$. We consider the morphism

$$\begin{aligned} \phi : F &\rightarrow \mathbb{P}^1 \\ (x,y) &\mapsto x \end{aligned}$$

From the Riemann-Hurwitz formula (since the genus of $\mathbb{P}^1$ is 1), we have that

$$2g(F) - 2 = -2 \deg \phi + \sum_{P \in F} (e_\phi(P) - 1), \tag{1}$$

and we have to find the degree and ramification points of ϕ. We have that

$$\deg \phi = [\overline{K}(F) : \overline{K}(\mathbb{P}^1)] = [\overline{K}(x,y) : \overline{K}(x)] = n$$

since $y = \sqrt[n]{1-x^n}$.

We now compute the ramification. For any $Q \in \mathbb{P}^1$, we have that

$$n = \deg \phi = \sum_{\phi(P)=Q} e_\phi(P). \tag{2}$$

For any affine point $Q = x_0$, we have that $\phi(P) = Q$ if $P = (x_0, y_0) \in F(\overline{K})$, which means that y_0 satisfies $y_0^n = 1 - x_0^n$. If $x_0^n \neq 1$, there are exactly n solutions, as $\overline{K}$ contains the nth roots of 1, and from (2), we get that $e_\phi(P) = 1$ for all such points P. If If $x_0^n = 1$, then there is only one point $P = (x_0, 0)$ such that $\phi(P) = Q$, and from (2), we get that $e_\phi(P) = n$. Since there are n values of x_0 such that $x_0^n = 1$, this gives that for the affine points $P \in F$, we have that

$$\sum_{P \in F} (e_\phi(P) - 1) = n(n-1).$$

We now find the points at infinity on F. Homegenizing and setting $Z = 0$, we have

$$X^n + Y^n = 0 \iff X^n = -Y^n \iff Y = \sqrt[n]{-1}X,$$

which gives the n points $[1, \zeta, 0]$ at infinity, where ζ is any of the nth roots of -1. Then, $\phi^{-1}([1,0])$ contains n points, and there is no ramification at infinity. This gives replacing in (1) that

$$2g(F) - 2 = -2(n) + n(n-1) \Rightarrow g(F) = \frac{(n-1)(n-2)}{2}.$$

(b) We consider the morphism

$$\begin{aligned} \phi : C &\rightarrow \mathbb{P}^1 \\ (x,y) &\mapsto x \end{aligned}$$

From the Riemann-Hurwitz formula (since the genus of $\mathbb{P}^1$ is 1), we have that

$$2g(E) - 2 = -2 \deg \phi + \sum_{P \in E} (e_\phi(P) - 1),$$

and we have to find the degree and ramification points of ϕ. We have that

$$\deg \phi = [\overline{K}(C) : \overline{K}(\mathbb{P}^1)] = [\overline{K}(x,y) : \overline{K}(x)] = 2$$

since $y = \sqrt{f(x)}$.

We now compute the ramification. For $x_i \in \mathbb{P}^1$, we have that $t_{x_i} = x - x_i$ and we have to compute $v_P(x - x_i)$ as a function in $\overline{K}(E)$, where $P = (x_i, y_i)$. As done before for elliptic curves, this gives for the affine points

$$v_P(x - x_i) = \begin{cases} 1 & P = (x_i, y_i), f(x_i) \neq 0 \\ 2 & P = (x_i, y_i), f(x_i) = 0 \end{cases}$$

Then, there are d affine ramification points, namely the points $P_i = (x_i, 0)$ where $f(x_i) = 0$, and we have $e_\phi(P_i) = 2$.

To compute the ramification at infinity, we use a previous assignment which showed that C has 2 points at infinity when d is even, and one when d is odd, i.e.

$$\#\phi^{-1}([1,0]) = \begin{cases} 2 & 2 \mid \deg(d) \\ 1 & 2 \nmid \deg(d), \end{cases}$$

and there is ramification at infinity only when d is odd.

This gives

$$2g(C) - 2 = \begin{cases} -2(2) + d & 2 \mid d \\ -2(2) + d + 1 & 2 \nmid d \end{cases}$$

and

$$g(C) = \left\lfloor \frac{d-1}{2} \right\rfloor .$$

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

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

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 $\#E_{\mathrm{ns}}(\mathbb{F}_p)$ is

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

Solution from David Marcil: Firstly, note that we know that $E(K)$ must have at most one singular point. Then, by performing a change of coordinate (defined over K), we can assume that this point is at the origin. This is clearly a group automorphism. Indeed, we see that the point at infinity is fixed and one readily sees that the group law is respected by looking at its geometrical definition. Moreover, the slopes of the tangent lines in the original curve at our singular points are defined over K if and only if the slopes of the tangent lines of our new curve at the origin are defined over K, and the type of the singularity (node or cusp) is also preserved, hence we can solve the question entirely by assuming the singular point is at the origin.

That being said, since $(0, 0)$ is a singularity, we know that E is given by a singular Weierstrass equation of the form $y^2 + a_1xy = x^3 + a_2x^2$, hence the tangents are given by $y^2 + a_1xy - a_2x^2 = (y - \alpha_1 x)(y - \alpha_2 x)$.

a) By looking at this last equation we know $\alpha_1 + \alpha_2 = -a_1 \in K$, so if α_1 is in K, we know that α_2 is as well. It follows that one can perform the change of coordinate (defined over K) $y \mapsto y + \alpha_1 x$. After this step, we can then follow the exact same step as in the original proof of Silverman (see Theorem 2.5 of Chapter 3) to conclude that $E_{ns}(K) \cong K^\times$. Moreover, the fact that $y^2 + a_1xy - a_2x^2 = (y - \alpha_1 x)(y - \alpha_2 x)$ implies that $(s - \alpha_1)(s - \alpha_2) = s^2 + a_1 s - a_2$ (simply let $s = y/x$), so α_1, α_2 both solve the same quadratic polynomial, i.e. $L = K(\alpha_1, \alpha_2)$ is a quadratic extension of K. Then, the slopes of the tangent at the origin are defined over L, so our previous work gives us that $E_{ns}(K) \subset E_{ns}(L) \cong L^\times$.

If $P = (x, y) \in E_{ns}(K)$, then by construction of the isomorphism $E_{ns}(L) \cong L^\times$, we know P corresponds to $\ell = \dfrac{y - \alpha_1 x}{y - \alpha_2 x}$. Since L/K is quadratic, it is Galois. Let σ the non-trivial automorphism in Gal(L/K), then

$$\sigma(\ell) = \frac{y - \sigma(\alpha_1)x}{y - \sigma(\alpha_2)x} = \frac{y - \alpha_2 x}{y - \alpha_1 x} = \ell^{-1}.$$

Therefore, $N_{L/K}(\ell) = \ell \cdot \sigma(\ell) = 1$.

Conversely, suppose $\ell \in L^\times$ such $N_{L/K}(\ell) = 1$. We know ℓ corresponds to some $P = (x, y) \in E_{ns}(L)$, hence $\ell = \dfrac{y - \alpha_1 x}{y - \alpha_2 x}$. Since $N_{L/K}(\ell) = 1$, we must have $\sigma(\ell) = \ell^{-1} = \dfrac{y - \alpha_2 x}{y - \alpha_1 x}$. On the other hand, we know $\sigma(\ell) = \dfrac{\sigma(y) - \alpha_2\sigma(x)}{\sigma(y) - \alpha_1\sigma(x)}$. By combining both facts, we find

$$\begin{aligned} &(\sigma(y) - \alpha_1\sigma(x))(y - \alpha_2 x) = (\sigma(y) - \alpha_2\sigma(x))(y - \alpha_1 x) \\ \implies\ & \alpha_1\sigma(x)y + \alpha_2\sigma(y)x = \alpha_2\sigma(x)y + \alpha_1\sigma(y)x \\ \implies\ & (\alpha_2 - \alpha_1)\sigma(x)y = (\alpha_2 - \alpha_1)\sigma(y)x \\ \implies\ & \sigma\left(\frac{x}{y}\right) = \frac{x}{y} \qquad (\text{as } \alpha_1 \neq \alpha_2) \end{aligned}$$

It follows that $x/y \in K$. Moreover, we can use the fact that $P \in E(L)$, i.e. $y^2 + a_1xy = x^3 + a_2x^2$ to divide by x^2 (which we can do since the only point with $x = 0$ is $(0, 0)$ which is the singular point, i.e. not in $E_{ns}(L)$) and obtain $x = \left(\frac{y}{x}\right)^2 + a_1\left(\frac{y}{x}\right) - a_2 \in K$. Therefore, $x \in K$, $y = (y/x) \cdot x \in K$, so $P \in E_{ns}(K)$. This shows that $E_{ns}(K) = \{\ell \in L^\times : N_{L/K}(\ell) = 1\}$.

b) If there is only one tangent, then it is given by $y^2 + a_1xy - a_2x^2 = (y - \alpha_1 x)^2$, which yields $2\alpha_1 = -a_1 \in K$, so $\alpha_1 \in K$. Therefore, we can again apply the transformation of coordinate (defined over K) $y \mapsto y + \alpha_1 x$ and perform the same proof as Silverman to conclude that $E_{ns}(K) \cong K^+$.

c) If $K = \mathbb{F}_p$ (then $L = \mathbb{F}_{p^2}$), then K^+ contains p elements and $K^\times$ contains $p - 1$ elements. Moreover, $N_{L/K} : \mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times$ is a group homomorphism with kernel $\{\ell \in L^\times : N_{L/K}(\ell) = 1\}$. It is surjective since, given $k \in \mathbb{F}_p$, we know we can find $l \in \mathbb{F}_{p^2}$ with norm k by solving $x^2 - k$. But $\mathbb{F}_{p^2}$ is the unique quadratic extension of $\mathbb{F}_p$, hence such an l must exist. It follows that $\{\ell \in L^\times : N_{L/K}(\ell) = 1\}$ contains exactly $(p^2 - 1)/(p - 1) = p + 1$ elements. Therefore, using part (a) and (b), we can conclude that the number of point in $E_{ns}(K)$ is exactly given by the formula stated in the question.

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

$$F(X_0, X_1, X_2) = X_1^2X_2 - X_0^3 - AX_0X_2^2 - BX_2^3 = 0,$$

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.

Solutions:

(a) By definition of the group structure.

(b) The determinant of the Hessian matrix is

$$24AX_0^2X_2 + 72BX_0X_2^2 + 24X_0X_1^2 - 8A^2X_2^3.$$

Then, it vanishes at the point at infinity, which is a 3-torsion point. For the affine points, using $X_2 = 1$, and renaming $X_0 = x$ and $X_1 = y$ such that the affine part of curve is $y^2 = x^3 + Ax + B$, the determinant of the Hessian at (x, y) is

$$8(3Ax^2 + 9Bx + 3xy^2 - A^2) \quad = \quad 8\left(3x^4 + 6Ax^2 - 12Bx - A^2\right). \tag{3}$$

We now use the formula for $P + P$. Let $P = (x, y)$ and $P + P = (w, z)$. In the notation of Silverman, we have that

$$\lambda = \frac{3x^2 + A}{2y}, \quad w = \lambda^2 - 2x.$$

P is a non-trivial 3-torsion point iff $P+P=-P$, which happen iff $w=x$ (since the 2 points with $w=x$ are P and $-P$, but $P+P\neq P$ since $P\neq\mathcal{O}$). Solving $x=\lambda^2-x \iff 3x=\lambda^2$ gives

$$3x=\frac{9x^4+6Ax^2+A^2}{4x^3+4Ax+4B} \iff 3x^4+6Ax^2+12Bx-A^2=0. \tag{4}$$

Comparing (3) and (4), this proves the result.

(c) By 2-torsion points are the intersection of the 2 cubics

$$\begin{aligned} X_1^2X_2-X_0^3-AX_0X_2^2-BX_2^3 &= 0\\ 24AX_0^2X_2+72BX_0X_2^2+24X_0X_1^2-8A^2X_2^3 &= 0, \end{aligned}$$

so by Bezout's theorem, there are 9 of them, counting multiplicity. If we set $x_2=0$, there is only one solution, namely $\mathcal{O}=[0,1,0]$, of multiplicity 1. We must then show that there are 8 distinct affine solutions (x,y). For each x satisfying $p(x)=3x^4+6Ax^2-12Bx-A^2=0$, there are 2 solutions $(x,\pm\sqrt{x^3+AX+B})$, so we must show that $p(x)$ has distinct roots. We compute $\mathrm{Res}(p,p')$ which is a multiple of $4A^3+27B^2$, so it is not zero.

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.