Elliptic curves. Fall 2018

Partial Solutions to Assignment 2. Due Wednesday October 3.

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 that Propostion 1.2 and Theorem 2.3 (of Chapter II in Silverman) are true for $C = \mathbb{P}^1$ and $C_1 = C_2 = \mathbb{P}^1$ respectively.

(a) Proposition 1.2: Show that $f \in \overline{K}(\mathbb{P}^1), f \neq 0$ has only finitely many zeroes and poles. Furthermore, if f has no poles, then f is a constant.

(b) Proposition 2.3: Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism. Then ϕ is either constant or surjective.

2. Show that Theorem 2.3 (of Chapter II in Silverman) is true when C_1, C_2 are plane curves given by a single equation.

Hint: Use the resultant of homogeneous polynomials with respect to different variables.

3. Let $C : F(X, Y, Z) = 0$ be a plane curve given by a single equation. Show that a point P is smooth if and only if M_P is a principal ideal.

Solutions: After a linear change of variable, we can assume that the smooth point is $(0, 0)$. Let $f(x, y) = 0$ be an affine model where $P = (0, 0)$ is the smooth point and $f(0, 0) = 0$. We want to show that the ideal $M_P = (x, y)$ in $\overline{K}[C]_P$ is principal. Since P is smooth, either

$$\frac{\partial f}{\partial x}(0,0) \neq 0, \quad \text{or} \quad \frac{\partial f}{\partial y}(0,0) \neq 0.$$

Wlog, say $\frac{\partial f}{\partial y}(0, 0) = \delta \neq 0$, and writing the Taylor expansion at $P = (0, 0)$, we have

$$f(x, y) = \frac{\partial f}{\partial x}(0,0)x + \delta y + \text{higher order terms} = \sum_{i=1}^{n} b_i x^i + y(\delta + g(x, y)),$$

where $g(x, y) \in \overline{K}[x, y]$, and $g(0, 0) = 0$. Then,

$$y(\delta + g(x, y)) = -\sum_{i=1}^{n} b_i x^i,$$

and $\delta + g(x,y)$ is a unit in $\overline{K}[C]_P$. This gives $y \in xM_P$, and $M_P = (x)$.

Conversly, assume that $M_P = (x,y)$ is generated by a single element, say z. Then, we have the equations

$$ux + vy = z, \quad x = zs, \quad y = zr,$$

for $u, v, s, r \in \overline{K}[C]_P$, and then $us + vr = 1$. Then, either r or s is a unit in $\overline{K}[C]_P$, wlog say that s is a unit. Since $rx - sy = 0$ in $\overline{K}[C]_P$ we can find polynomials $r(x,y)$, $s(x,y)$ and $g(x,y)$ in $\overline{K}[x,y]$, where $s(x,y)$ has non zero constant term, such that

$$f(x,y)g(x,y) = r(x,y)x - s(x,y)y$$

By comparing the coefficient of y on both sides, we conclude that

$$\frac{\partial f}{\partial y}(0,0) \neq 0.$$

Another proof using Proposition I.1.7:
Suppose that $M_P = (t)$ is a principal ideal in $\overline{K}[C]_P$. Then, the map

$$\begin{array}{rcl} \phi : \overline{K}[C]_P & \to & M_P/M_P^2 \\ f & \mapsto & ft \end{array}$$

is a surjective homorprphism of $\overline{K}$-verctor space with kernel M_P. From Hilbert NullStellenSatz, we have that

$$\overline{K}[C]_P/M_P \simeq \overline{K} \simeq M_P/M_P^2,$$

and the result follows from Proposition I.1.7.

4. Let K be a field of characteristic different than 2. Let E/K be the curve with affine equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in K$.

(a) Show that E is isomorphic to a curve $y^2 = x^3 + px + q$, which is non-singular if and only if $4p^3 + 27q^2 \neq 0$. We suppose from now on that E is non-singular.

(b) Show that the rational map ϕ defined on E by $\phi(x,y) = (x, -y - a_1x - a_3)$ is an isomorphism.

(c) Let $f \in K(E)$ and $\phi^* f = f \circ \phi$. Let $P \in E(K)$, $Q = \phi(P)$ and t_Q be a uniformizer at Q. Show that $\phi^* t_Q$ is a uniformizer at P and $v_Q(f) = v_P(\phi^* f)$.

Solutions: (a) Seen in class.

(b) We have a rational map between non-singular curves, it is then a morphism. Also, $\phi^{-1} = \phi = (x, -y - a_1 x - a_3)$ is the inverse of ϕ, so ϕ is an isomorphism.

(c) Since ϕ is an isomorphism, ϕ^* is an field isomorphism of $\overline{K}(E)$. Since $(\phi^* f)(P) = f(\phi(P)) = f(Q)$, we have that ϕ^* is an isomorphism between the local rings $\overline{K}(E)_P$ and $\overline{K}(E)_Q$. Then, $\phi^* t_Q$ is a uniformizer at P and $v_Q(f) = v_P(\phi^* f)$. We remark that the result is also a particular case of **3.** taking $f = t_Q$ since $e_\phi(P) = 1$ for any P because ϕ is an isomorphism.

5. Let E be a curve as in **4.**. Let $f \in K(E)^*$. Show that $\deg(\mathrm{div}(f)) = 0$ by following the steps:

(a) Show that the result hold for $f(x) = (x - x_i)$, and then for any polynomial $a(x) \in K(E)$.

(b) Show that result hold for $f(x, y) = a(x) + yb(x)$. *Hint:* Use the map ϕ of **4.**(b)

(c) Show that the result hold for a general $f \in K(E)$.

Solutions: (a) Let's suppose that $\mathrm{char}(K) \neq 2$, and write $E : y^2 = f(x)$. Let $P = (x_i, y_i)$ be an affine point on E. Then, there are 2 points $P \in E(\overline{K})$ with x-coordinate $x = x_i$, namely $P^{\pm} = (x_i, \pm\sqrt{f(x_i)})$ and they are equal if and only if $f(x_i) = 0$ if and only if x_i is a root of $f(x)$. The uniformizer at $P = (x_i, y_i)$ is

$$\begin{aligned} t_P &= (x - x_i) \quad \text{if } x_i \text{ is not a root of } f(x) \\ t_P &= y \quad \text{if } x_i \text{ is not a root of } f(x) \end{aligned}$$

The uniformizer for x_i a root of $f(x)$ was done in class, and to show that $x - x_i$ is a uniformizer at $P_i = (x_i, y_i)$ when x_i is not a root of $f(x) = x^2 + Ax + B$, we use

$$(y - y_i)(y + y_i) = y^2 - y_i^2 = x^3 + Ax + B - (x_i^3 + AX_i + B) = (x - x_i)(x^2 + xx_i + x_i^2 + A).$$

So,

$$y - y_i = \frac{(x - x_i)(x^2 + xx_i + x_i^2 + A)}{y + y_i},$$

and $(x - x_i)$ is the uniformizer. In the first case, $v_{P^+}(x - x_i) = v_{P^-}(x - x_i) = 1$, and in the second case, $P = P^+ = P^-$ and $v_P(x - x_i) = 2$. In both cases, we have that $v_{\mathcal{O}}(x - x_i) = 2$, Indeed, homogenizing

$$x - x_i = \frac{x - x_i z}{z},$$

and evaluating at $\mathcal{O} = [0, 1, 0]$, we get that

$$\mathrm{ord}_{\mathcal{O}}(x - x_i) = \mathrm{ord}_{\mathcal{O}}(x - zx_i) - \mathrm{ord}_{\mathcal{O}}(z),$$

and using the equation for the dehomogenization with $y = 1$, we get

$$z = (x - e_1 z)(x - e_2 z)(x - e_3 z),$$

and $\mathrm{ord}_{\mathcal{O}}(z) = 3$. We also have that $\mathrm{ord}_{\mathcal{O}}(x - zx_i) = 1$, which gives $\mathrm{ord}_{\mathcal{O}}\left(\frac{x - zx_i}{z}\right) = -2$. Finally, we showed that

$$\mathrm{div}(x - x_i) = (P^+) + (P^-) - 2(\mathcal{O}),$$

where $P^+ = P^-$ if and only if $f(x_i) = 0$. Then, $\deg \mathrm{div}(x - x_i) = 0$.

For any polynomial $a(x)$, we can write $a(x) = \prod_{i=1}^d (x - x_i)^{n_i}$, which gives that

$$\mathrm{div}\ a(x) = \sum_{i=1}^d n_i \mathrm{div}(x - x_i) = \sum_{i=1}^d n_i(P_i^+) + n_i(P_i^-) - 2n_i(\mathcal{O}), \tag{1}$$

which is a divisor of degree 0.

(b) We now consider a function $a(x) + yb(x)$, and the map

$$\begin{aligned} \phi : E \quad &\to E \\ (x, y) \quad &\mapsto \quad (x, -y) \end{aligned}$$

Then, we have that

$$v_P\left(a(x) + yb(x)\right) = v_{\phi(P)}\left(a(x) - yb(x)\right)$$

for all $P \in E(\overline{K})$, where $P, \phi(P)$ where denoted by $P^{\pm}$ in (a). Hence, it follows from (1) that

$$\mathrm{div}\left(a(x) + yb(x)\right) = \sum_P n_P(P) \iff \mathrm{div}\left(a(x) - yb(x)\right) = \sum_P n_P(\phi(P)),$$

and $\deg \operatorname{div}(a(x)+yb(x)) = \deg \operatorname{div}(a(x)-yb(x))$. Now,

$$(a(x)+yb(x))(a(x)-yb(x)) = a^2(x) - y^2b^2(x) = a^2(x) - f(x)b^2(x)$$

is independent of y, and by (a)

$$\begin{aligned} 0 &= \deg \operatorname{div}(a(x)+yb(x))(a(x)-yb(x)) \\ &= \deg \operatorname{div}(a(x)+yb(x)) + \deg \operatorname{div}(a(x)-yb(x)) = 2\deg \operatorname{div}(a(x)+yb(x)), \end{aligned}$$

and $\deg \operatorname{div}(a(x)+yb(x)) = 0$.

(c) Now, any function in the function field $\overline{K}(E) = \overline{K}[x,y]/(y^2 - f(x))$ can be written as $g(x,y)/h(x,y)$, where $g(x,y), h(x,y) \in \overline{K}[x,y]$. Supoose that $\deg g = 2n$ is even (the proof for odd is identical). Then,

$$\begin{aligned} g(x,y) &= \sum_{i=0}^{2n} b_i(x)y^i = \sum_{i=0}^{n} b_{2i}y^{2i} + \sum_{i=0}^{n-1} b_{2i+1}(x)y^{2i+1} \\ &= \sum_{i=1}^{n} b_{2i}(x)f(x)^i + y\sum_{i=1}^{n-1} b_{2i+1}(x)f(x)^i = a(x) + yb(x), \end{aligned}$$

and similarly for $h(x,y)$. We have proven that any function in the function field $\overline{K}(E) = \overline{K}[x,y]/(y^2 - f(x))$ writes as

$$\frac{a_1(x) + yb_1(x)}{a_2(x) + yb_2(x)},$$

and the results follows from (b).

6. (Silverman II.2.2) Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves, $f \in \overline{K}(C_2)^*$, $P \in C_1$. Show that

$$\operatorname{ord}_P(\phi^* f) = e_\phi(P) \operatorname{ord}_{\phi(P)}(f).$$

Solutions: Let $t_{\phi(P)} \in \overline{K}(C_2)$ be a unformizer at $\phi(P)$, and let $f \in \overline{K}(C_2)_{\phi(P)}$. Since $\overline{K}(C_2)_{\phi(P)}$ is a DVR, we can write $f = t^k_{\phi(p)}u$, where $v_{\phi(p)}(u) = 0$. Then, $\phi^* g = (\phi^* t_{\phi(P)})^k \phi^* u$, and by definition, $\operatorname{ord}_P(\phi^* u) = \operatorname{ord}_{\phi(P)} u = 0$. Then,

$$\operatorname{ord}_P(\phi^* f) = \operatorname{ord}_P((\phi^* t_{\phi(p)})^k \phi^* u) = k \operatorname{ord}_P(\phi^* t_{\phi(p)}) = \operatorname{ord}_{\phi(P)}(f)\ e_\phi(P).$$

7. (Silverman II.2.14)

Solution from Reginald Lybbert:

Question 7: *For this exercise we assume that char $K \neq 2$. Let $f(x) \in K[x]$ be a polymonial of degree $d \geq 1$ with nonzero discriminant, let C_0/K be the affine curve given by the equation:*

$$C_0 : y^2 = f(x) = a_0x^d + a_1x^{d-1} + \ldots + a_{d-1}x + a_d$$

and let g be the unique integer satisfying $d - 3 < 2g \leq d - 1$.

(a) *Let C be the closure of the image of C_0 via the map*

$$[1, x, x^2, \ldots, x^{g+1}, y] : C_0 \to \mathbb{P}^{\eth+\nvDash}$$

Prove that C is smooth and tthat $C \cap \{X_0 \neq 0\}$ is isomorphic to C_0.

We see that the ideal of the image of C_0 via the map mentioned contains the following set of homogeneous polynomials.

$$\mathcal{F} := \{X_iX_j - X_pX_q : i + j = p + q, 0 \leq i, j, p, q \leq g + 1\}$$

along with the polynomial.

$$H : X_{g+2}^2X_0^{d-2} \quad -(a_0X_1^d + a_1X_1^{d-1}X_0 + \ldots + a_{d-1}X_1X_0^{d-1} + a_dX_0^d)$$

Note that the image of these polynomials is bigger than C_0 since it contains the hyperplane $X_0 = X_1 = 0$. Thus, we must remove this, by substituting some of the equations of $\mathcal{F}$ into H to get (in the case d is even):

$$H : X_{g+2}^2X_0^{d-2} - a_0X_{g+1}^2X_0^{d-2} - a_1X_gX_{g+1}X_0^{d-2} - \ldots - a_{d-1}X_1X_0^{d-1} - a_dX_0^d$$

or in the case d is odd:

$$H : X_{g+2}^2X_0^{d-2} - a_0X_{g+1}X_gX_0^{d-2} - a_1X_g^2X_0^{d-2} - \ldots - a_{d-1}X_1X_0^{d-1} - a_dX_0^d$$

Either way, we can now reduce the degree of this polynomial by removing a factor of X_0^{d-2}. This gives us H_{even} if d is even, or H_{odd} if d is odd.

$$\begin{aligned} H_{even} : X_{g+2}^2 &\quad -(a_0 X_{g+1}^2 + a_1 X_{g+1} X_g + \ldots + a_{d-1} X_1 X_0 + a_d X_0^2) \\ H_{odd} : X_{g+2}^2 &\quad -(a_0 X_{g+1} X_g + a_1 X_g^2 + \ldots + a_{d-1} X_1 X_0 + a_d X_0^2) \end{aligned}$$

Let C be the variety corresponding to the ideal generated by $\mathcal{F}$ and $\hat{H}$, where $\hat{H} = H_{even}$ or H_{odd}, depending on the parity of d.

Now, if we set $X_0 \neq 0$, we see that the only possible solutions to this correspond exactly to C_0. Let P be a projective point that satisfies all of these equations, with $X_0 \neq 0$. Then, we can scale to get a representative where $X_0 = 1$. Then set $X_1 = x$, and then, by equation $X_i X_0 = X_{i-1} X_1 \in \mathcal{F}$, $X_i = x^i$. Then, this causes H to become exactly the equation for C_0. Thus, the affine part of C where $X_0 \neq 0$ is exactly the image of C_0. It remains to show that C is non-singular at the parts where $X_0 = 0$.

Suppose $X_0 = 0$, Suppose that $X_{i-1} = 0$ for some $0 < i < g+1$. Then $X_i^2 = X_{i-1} X_{i+1}$ is an equation in $\mathcal{F}$. So, since $X_{i-1} = 0$, we must have $X_i = 0$. Thus, by induction we see that if $X_0 = 0$, then $X_i = 0$ for all $i < g+1$.

Now, if d is odd, this reduces the equation H to X_{g+2}^2. So $X_{g+2} = 0$. So, we have only one point at infinity, namely $[0, 0, \ldots, 0, 1, 0]$. So, let us dehomogenize C using $X_{g+1} = 1$. Then, using the equation $X_{g+1} X_{g-i} = X_g X_{g-i+1}$, we see that $X_{g-i} = X_g^{i+1}$, for all $0 \leq i \leq g$. So, call $X_g / X_{g+1} = v$, and $X_{g+2}/X_{g+1} = u$. This gives us the equation:

$$u^2 = a_0 v + a_1 v^2 + \ldots + a_d v^d + a_d v^{d+1}$$

However, since $f(x)$ had non-zero discriminant, we see that the polynomial $a_0 + a_1 x + \ldots + a_d x^d$ has no double roots, and since $a_0 \neq 0$, we also have $a_0 v + a_1 v^2 + \ldots + a_d v^{d+1}$ having no double roots. Therefore, the above equation gives a smooth curve. Thus C is smooth, when d is odd.

On the other hand, if d is even, H reduces to $X_{g+2}^2 = a_0 X_{g+1}^2$. Here, we have two points at infinity, namely $[0, 0, \ldots, 0, 1, \pm\sqrt{a_0}]$. Note that $\sqrt{a_0} \neq 0$, since $f(x)$ is exactly degree d. Now, we again homogenize at $X_{g+1} = 1$. Using the same equations as before, we still have $X_{g-i} = X_g^{i+1}$, so setting $v = X_g / X_{g+1}$, and $u = X_{g+2}/X_{g+1}$, we get:

$$u^2 = a_0 + a_1 v + \ldots + a_d v^d$$

Then, since $f(x)$ had non-zero discriminant, we see that it had no double roots. So, if we homogenize f and dehomogize with respect to the other variable, we still have no double roots. But that is exactly what it here. Thus, $a_0+a_1v+\ldots+a_dv^d$ has no double roots. Therefore, the above equation describes a smooth affine curve. Therefore, C is smooth, when d is even.

(b) *Let*

$$f^*(v) = v^{2g+2}f(1/v) = \begin{cases} a_0 + a_1 v + \ldots + a_{d-1}v^{d-1} + a_d v^d & \text{if } d \text{ is even} \\ a_0 v + a_1 v^2 + \ldots + a_{d-1}v^d + a_d v^{d+1} & \text{if } d \text{ is odd} \end{cases}$$

Show that C consists of two pieces:

$$C_0 : y^2 = f(x) \qquad \text{and} \qquad C_1 : u^2 = f^*(v)$$

"glued together" via the maps

$$\begin{array}{cc} C_0 \to C_1 & C_1 \to C_0 \\ (x,y) \mapsto (1/x, y/x^{g+1}) & (v,u) \mapsto (1/v, u/v^{g+1}) \end{array}$$

Using exactly the dehomogenizations is the last part, we have already shown that C consists of C_0 and C_1. Note that C_0 contains all but one or two of the points of C, but those points are shown to be in C_1, thus these are the only two pieces necessary. It remains to compute the gluing data.

We need only consider points on C that are on both the affine part of C_0, (where $X_0 \neq 0$), and the affine part of C_1,(where $X_{g+1} \neq 0$). Now, using the coordinates of C_0, we see that $X_{g+1} = x^{g+1}$. Thus $v = X_g/X_{g+1} = x^g/x^{g+1} = 1/x$, Also, $w = X_{g+2}/X_{g+1}$ so $w = y/x^{g+1}$. Thus, the gluing map $C_0 \to C_1$ is $(x,y) \to (1/x, y/x^{g+1})$.

Now, to look at the other direction, recall that using the coordinates of C_1, we have $X_0 = v^{g+1}$. Thus $x = X_1/X_0 = v^g/v^{g+1} = 1/v$, and $y = X_{g+2}/X_0 = u/v^{g+1}$. Thus, the gluing map $C_1 \to C_0$ is $(v,u) \to (1/v, u/v^{g+1})$.

8. (Silverman II.2.15))

9. (Silverman II.2.16) Let C/K be a curve that is defined over K and let $P \in C(K)$. Prove that $K(C)$ contains uniformizers for C at P, i.e. prove that there are uniformizers that are defined over K.

Solution from Martin C̃ech:

Let t_P be a uniformizer at P. Then t_P is defined over some field M which is a finite extension of K. We will assume that the extension M/K is separable, and denote by L the normal closure of M, so that L/K is finite and Galois.

In general, every uniformizer at P is of the form ut_P for a unit $u \in \overline{K}[C]_P$. Let $\sigma_1, \dots, \sigma_k$ denote all the elements of $\mathrm{Gal}(L/K)$. Then for every $i = 1, \dots, k$, $\sigma_i(t_P) = u_i \cdot t_P$ for some unit $u_i \in L[C]_P$ – we would like to find a unit $v \in L[C]_P$ such that $\sigma_i(vt_P) = vt_P$, which would imply (by the exercise from previous assignment) that vt_P is a uniformizer defined over K.

Since we know that $\sigma_i(vt_P) = \sigma_i(v)u_it_P$, we need this unit v to satisfy $u_i = \frac{v}{\sigma_i(v)}$ for every i. We can find such a v using Hilbert's Theorem 90.

The map $\phi: \ \sigma_i \mapsto u_i$ is a 1-cocycle with values in $L[C]_P^\times$, since $\sigma_i\sigma_j(t_P) = \sigma_i(u_jt_P) = \sigma_i(u_j)u_it_P$, so $\phi(\sigma_i\sigma_j) = u_i\sigma_i(u_j)$. Since $L[C]_P$ is an (infinite dimensional) vector space over L, we can use Hilbert's Theorem 90 and a similar prove as in the last exercise of the last assignment to show that $H^1(\mathrm{Gal}(L/K), L[C]_P^\times) = 1$. This shows that ϕ is a 1-coboundary, so is of the form $\phi(\sigma_i) = u_i = \frac{\sigma_i(w)}{w}$ for some w. Setting $v = w^{-1}$, we have $\frac{v}{\sigma_i(v)} = \frac{\sigma_i(w)}{w} = u_i$ as we wanted.