Elliptic Curves Example Sheet 1

Isaac Martin

Last compiled February 10, 2022

EXERCISE 2 Find rational parametrizations for the plane conic $x^2+xy+3y^2=1$ and for the singular plane cubic $y^2=x^2(x+1)$.

Proof: We first consider the plane conic $f(x,y)=x^2+xy+3y^2-1=0$ as a curve over $\mathbb{R}$, and we illustrate the method by which the rational parametrization was found for the sake of the author who will revise these problems prior to the exam. The point $(-1,0)$ is a solution to $f(x,y)=0$ and therefore the line $y=t(x+1)$ intersects the curve defined by f at this point. We claim it intersects the ellipse f at exactly one other point for all but a single value of $t\in\mathbb{R}$. This point must satisfy the equation $f(x,t(x+1))=0$, hence

$$\begin{aligned} f(x,t(x+1)) &= x^2+x(t(x+1))+3(t(x+1))^2-1=0 \\ &\iff (x^2-1)+x(t(x+1))+3(t(x+1))^2=0 \\ &\iff (x+1)\left[(x-1)+xt+3t^2(x+1)\right]=0 \\ &\iff x=-1 \quad \text{or} \quad x=\frac{1-3t^2}{1+t+3t^2}. \end{aligned}$$

Using the latter expression to solve for y in terms of t gives us the potential parameterization

$$x_t=\frac{1-3t^2}{1+t+3t^2},\ y_t=\frac{2t+t^2}{1+t+3t^2}.$$

The calculation above proves that $f(x_t,y_t)=0$, so we need only show that $t\mapsto(x_t,y_t)$ is injective outside of a finite subset of $\mathbb{R}$. To see this, consider the map $f(\mathbb{R}^2)\setminus\{(-1,0),(-1,1/3)\}\to\mathbb{A}^1$ defined $(x,y)\mapsto\frac{y}{x+1}$ is an inverse to $t\mapsto(x_t,y_t)$ outside except at $(-1,0)$ and $(-1,1/3)$. This means $t\mapsto(x_t,y_t)$ is injective except at these two points, and is therefore a rational parameterization of the curve.

Now consider the plane conic $C:\ y^2=x^2(x+1)$, and let $x_t=t^2-1$ and $y_t=t(t^2-1)$. I claim that $t\mapsto(x_t,y_t)$ is a rational parameterization of C. The map $(x,y)\mapsto y/x$ is an inverse to $t\mapsto(x_t,y_t)$ everywhere except $(x,y)\in\{(\pm1,1),(\pm1,-1),(0,0)\}$ since

$$\frac{t(t^2-1)}{(t^2-1)}=t \quad \text{when} \quad t\neq\pm1,$$

hence $t\mapsto(x_t,y_t)$ is injective outside a finite subset of $\mathbb{R}$. Furthermore,

$$y_t^2=t^2(t^2-1)^2=(t^2-1)^2(t^2-1+1)=x_t^2(x_t+1),$$

so $t\mapsto(x_t,y_t)$ is indeed a rational parameterization of C. □

EXERCISE 7 Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2=f(x)$.

(i) Put the curve $E_d:\ dy^2=f(x)$ in Weierstrass form.

(ii) Show that if $j(E) \neq 0, 1728$ then every twist of E is isomorphic to E_d for some unique square-free integer d. [A *twist* of E is an elliptic curve E' defined over $\mathbb{Q}$ that is isomorphic to E over $\overline{\mathbb{Q}}$.]

EXERCISE 9

(i) Find a formula for doubling a point on the elliptic curve $E: \ y^2 = x^3 + ax + b$. [You should fully expand the numerator of each rational function in your answer.]

(ii) Find a polynomial in x whose roots are the x-coordinates of the points T with $3T = 0_E$. [Hint: Write $3T = 0_E$ as $2T = -T$.]

(iii) Show that the polynomial found in *(ii)* has distinct roots.

Proof:

(i)

□

EXERCISE 10 Let C be the plane cubix $aX^3 + bY^3 + cZ^3 = 0$ with $a, b, c \in \mathbb{Q}^*$. Show that the image of the morphism $C \longrightarrow \mathbb{P}^3$; $(X^3 : Y^3 : Z^3 : XYZ)$ is an elliptic curve E, and put E in Weierstrauss form. [You should try to give an answer that is symmetric under permuting a, b and c.] What is the degree of the morphism from C to E?