Topics in Algebraic Geometry (Elliptic Curves)

Solution of HW #I by Mesut Sahin

Due Monday, Feb. 23, 2004

(1) Show that the map from the quartic $\mathcal{C}_1 : z^2 = x^4 + 1$ to the Weierstrass cubic $E_1 : u^2 = v^3 - 4v$ is defined for all points of a field except finitely many. Show that the same is true for the inverse map. Thus the map $\mathcal{C}_1 \to E_1$ is an example of a birational isomorphism (a map defined by rational functions, giving a bijection between the (complex) points on the curves except for finitely many exceptions).

Solution: Let (x, z) be a point of $\mathcal{C}_1$. Then $z^2 = x^4 + 1$ holds, in other words, we have $1 = z^2 - x^4 = (z - x^2)(z + x^2)$. Let $t = z + x^2$, which yields that $\frac{1}{t} = z - x^2$. Thus we get

$$2x^2 = \frac{(t^2 - 1)}{t}$$

from which (multiplying both sides by $8t^2$) follows that

$$16x^2t^2 = 8t^3 - 8t.$$

Setting $u = 4xt$ and $v = 2t$ we obtain $u^2 = v^3 - 4v$, i.e. the equation of E_1. Thus the map $\mathcal{C}_1 \to E_1$ can be defined by

$$u = 4x(z + x^2), v = 2(z + x^2).$$

Obviously it is rational (indeed, more than rational)[1]. By using the relations $(t = v/2, x = u/4t, z = t - x^2)$ above the converse map can be given by

$$x = \frac{u}{2v}, z = \frac{(2v^3 - u^2)}{4v^2}$$

unless $v = 0$. There is only one point (u, v) on E_1 where this map is not defined, namely the origin. Therefore $\mathcal{C}_1$ and E_1 are birationally equivalent.

[1] These maps are called polynomial.

(2) Transform the Fermat quartic $\mathcal{C}_2 : z^2 = x^4 - 4$ into Weierstrass form $E_2 : u^2 = v^3 + v$, and show that the map you find is a birational isomorphism.

Solution: Let (x, z) be a point of $\mathcal{C}_2$. Then $z^2 = x^4 - 4$ holds, or we have $4 = x^4 - z^2 = (x^2 - z)(x^2 + z)$. Let $4t = z + x^2$, which implies that

$$\frac{1}{t} = x^2 - z.$$

So we get

$$2x^2 = \frac{(4t^2 + 1)}{t}$$

from which (multiplying both sides by $2t^2$) follows that

$$4x^2t^2 = 8t^3 + 2t.$$

Setting $u = 2xt$ and $v = 2t$ we obtain $u^2 = v^3 + v$, i.e. the equation of E_2. Thus the map $\mathcal{C}_2 \to E_2$ can be defined by

$$u = \frac{x(z + x^2)}{2}, v = \frac{(z + x^2)}{2}.$$

Obviously it is rational (indeed, more than rational). By using the relations above the converse map can be given by

$$x = \frac{u}{v}, z = \frac{2v^3 - u^2}{v}$$

unless $v = 0$. There is only one point (u, v) on E_2 where this map is not defined, namely the origin. Therefore $\mathcal{C}_2$ and E_2 are birationally isomorphic.

(3) Consider the two 'curves' $C_1 : X^4 + Y^4 = Z^2$ and $C_2 : X^4 - 4Y^4 = Z^2$ occurring in the proof of FLT for exponent 4. In our proof we started with a rational point (x, y, z) on C_1 and obtained a rational point (a, b, x) on C_2. Express x, y, z as rational functions of a, b, x; this defines a rational map $\phi : C_2 \to C_1$.

Is the rational map that you get birational (i.e., can the converse map $C_1 \to C_2$ be expressed using rational functions)?

Solution: In the proof of FLT for exponent 4 we found that $y^2 = 4ab$ and $z = a^4 + 4b^4$. So letting

$$X(a, b, x) = x, Y(a, b, x) = 2ab, Z(a, b, x) = a^4 + 4b^4$$

gives us the rational map $\phi : C_2 \to C_1$. For the converse map there is only one candidate to be a rational map, namely the one given by

$$a^4 = \frac{1}{2}(z + x^2), b^4 = \frac{1}{8}(z - x^2), x(x, y, z) = x.$$

And there is no chance for this map to be a rational map. So C_1 and C_2 are <u>not</u> birationally equivalent.

(4) Consider the following diagram:

$$\begin{array}{ccc} C_2 & \longrightarrow & E_2 \\ {\scriptstyle\phi}\downarrow & & \\ C_1 & \longrightarrow & E_1 \end{array}$$

Since the horizontal maps are (essentially) bijective, you can define a map $\psi : E_2 \longrightarrow E_1$ (i.e. rewrite ϕ in terms of the new coordinates u, v). Do this.

Solution: Let us consider the following diagram:

$$\begin{array}{ccc} E_2 & \xrightarrow{\psi} & E_1 \\ \downarrow & & \uparrow \\ \mathcal{C}_2 & & \mathcal{C}_1 \\ \downarrow & & \uparrow \\ C_2 & \xrightarrow{\phi} & C_1 \end{array}$$

Now start with a point $(u, v) \neq (0, 0)$ on E_2, by second question we know that the point

$$(x, y) = (\frac{u}{v}, \frac{2v^3 - u^2}{v})$$

lies on $\mathcal{C}_2$. Let

$$x = \frac{X}{Y}, z = \frac{Z}{Y^2}$$

where $Y \neq 0$. Then it is "pretty" obvious that for any point (x, y) on $\mathcal{C}_2$ there corresponds a point (X, Y, Z) on C_2, in other words, $z^2 = x^4 - 4$ implies that $X^4 - 4Y^4 = Z^2$. And this point, by the third question, is mapped to the point

$$(X', Y', Z') = (Z, 2XY, X^4 + 4Y^4)$$

on C_1, i.e. $Z'^2 = X'^4 + Y'^4$. By defining

$$x' = \frac{X'}{Y'}, z' = \frac{Z'}{Y'^2}$$

where $Y' \neq 0$ we obtain the point (x', y') on $\mathcal{C}_1$ corresponding to (x, y). By the first question we will obtain the point (u', v') on E_1, as a rational function of u and v. To write this function down we use the following relations:

$$x' = \frac{X'}{Y'} = \frac{Z}{2XY} = \frac{2v^3 - u^2}{2uv},$$
$$z' = \frac{Z'}{Y'^2} = \frac{X^4 + 4Y^4}{4X^2Y^2} = \frac{u^4 + 4v^4}{4u^2v^2}.$$

By inserting these into the following equations we get the result:

$$u' = 4(x'z' + x'^3) = \frac{(2v^3 - u^2)(u^4 + 4v^4)}{2u^3v^3} + \frac{(2v^3 - u^2)^3}{2u^3v^3}$$
$$v' = 2(z' + x'^2) = \frac{(2v^3 - u^2)^2 + (u^4 + 4v^4)}{2u^2v^2}$$

which defines the rational function ψ on E_2 (except the origin).

Comments. [FL] This mess can be simplified considerably using the relation $u^2 = v^3 + v$. In fact,

$$v' = \frac{(2v^3 - u^2)^2 + (u^4 + 4v^4)}{2u^2v^2} = \frac{2u^4 - 4u^2v^3 + 4v^4 + 4v^6}{2u^2v^2}$$
$$= \frac{u^4 - 2u^2v^3 + 2v^3(v + v^3)}{u^2v^2} = \frac{u^4 - 2u^2v^3 + 2v^3u^2}{u^2v^2} = \frac{u^2}{v^2}.$$

Similarly,

$$u' = \frac{2v^3 - u^2}{uv}\,\frac{(u^4 + 4v^4) + (u^2 - 2v^3)^2}{2u^2v^2}$$
$$= \frac{u(2v^3 - u^2)}{v^3} = \frac{u(v - v^3)}{v^3} = \frac{u(v^2 - 1)}{v^2}.$$

(5) Show that $7 = a^3 + b^3$ for some *positive* rational numbers. Hint: starting with the point $P = (2, 1)$ on the cubic $C : x^3 - y^3 = 7$, construct the tangent to C at P and compute their point of intersection $Q \neq P$.

Solution: The equation of the tangent line L to

$$C : f(x, y) = x^3 - y^3 - 7 = 0$$

at $(2, 1)$ is given by

$$\frac{\partial f}{\partial x}\Big|_{(2,1)}(x - 2) + \frac{\partial f}{\partial y}\Big|_{(2,1)}(y - 1) = 0$$

which can be arranged as $L : y = 4x - 7$. By Bezout's Theorem the number of intersection points of "C and L" is 3 counting with multiplicity. Since this line is tangent to C at $(2, 1)$ the intersection multiplicity of "L and C" at $(2, 1)$ is 2. Let us now find the third intersection point by plugging $y = 4x - 7$ into the equation $x^3 - y^3 = 0$. Then the equation becomes

$$-63x^3 + 336x^2 - 588x + 336 = (x - 2)^2(63x - 84) = 0$$

Thus $x = \frac{4}{3}$ is one component of $Q \neq P$, and the other is $y = 4x - 7 = -\frac{5}{3}$. So we conclude that, for rational numbers $a = \frac{4}{3}$ and $b = \frac{5}{3}$ the equation $a^3 + b^3 = 7$ is satisfied.