Elliptic curves

Remarks on polynomials

November 24, 2009

1 An elliptic curve is defined as a smooth cubic curve in $\mathbb{P}^2_k$ with a k-point. In lectures we proved that every elliptic curve with a k-point which is a flex has a Weierstrass form. Here is the proof that *every elliptic curve over a field of characteristic different from* 2 *and* 3 *is isomorphic to an ellitpic curve in short Weierstrass form.*

Let $C \subset \mathbb{P}^2_k$ be a smooth cubic with a k-point P. If P is a flex we are done by a result from lectures, so suppose it is not. Then the tangent $T_{P,C}$ meets C at a point $Q \neq P$. Let us make a linear change of coordinates so that $P = (1 : 0 : 0)$ and $Q = (0 : 0 : 1)$. Then $T_{P,C}$ is given by $y = 0$. Then the equation of C is $xz^2 + yq(x, y, z) = 0$, where $q(x, y, z)$ is homogeneous of degree 2. In the affine plane $y = 1$ this becomes

$$z^2 l_1(x) + z l_2(x) + q(x, 1, 0) = 0,$$

where $l_1(x)$ is of degree 1, and $l_2(x)$ is of degree at most 1. After a linear change of variables $t = l_1(x)$ we get

$$z^2 t + z l(t) + m(t) = 0, \tag{1}$$

where $l(t)$ is linear and $m(t)$ is quadratic. Now multiply by $4t$ and complete a square, that is, let $u = 2tz + l(t)$. Then

$$u^2 = l(t)^2 - 4tm(t) \tag{2}$$

can be reduced to a short Weierstrass form because the right hand side is a cubic polynomial in t.

If you feel confident in algebraic geometry, check that the projective closures of the curves (1) and (2) are isomorphic. [Hint: the inverse map $z = (u - l(t))/2t$ is defined outside $t = 0$. But (2) implies that $(u - l(t))/2t = -2m(t)/(u + l(t))$ provided both fractions are defined. The map $z = -2m(t)/(u+l(t))$ sends the point $t = 0$, $u = l(t)$ to $z = -m(0)/l(0)$, and the point $t = 0$, $u = -l(t)$ to the point at infinity of (1) where $t = 0$. The point at infinity of (2) goes to the point at infinity of (1) where $z = 0$. These arguments can be used to cover both curves by open subsets and to exhibit polynomial maps that are inverses of each other.]

2 Let E be the elliptic curve

$$y^2 = G(x),$$

where $G(x) \in \mathbf{Z}[x]$ is a separable cubic polynomial. For $(x', y') = 2(x, y)$ the duplication formula gives

$$x' = \frac{F(x)}{4G(x)} = \frac{G'(x)^2 - 8xG(x)}{4G(x)}.$$

Since $G(x)$ is separable, $F(x)$ and $G(x)$ are coprime in $\mathbf{Q}[x]$. Euclid's algorithm then produces polynomials $Q(x)$, $C(x) \in \mathbf{Z}[x]$ of degrees 2 and 3, respectively, such that $F(x)Q(x) + 4G(x)C(x) = c$, for some constant $c \in \mathbf{Z}$. We homogenize all these polynomials and so obtain

$$F(x, y)yQ(x, y) + 4yG(x, y)C(x, y) = cy^7.$$

Hence we obtain homogenous forms $A(x, y)$ and $B(x, y)$ with integral coefficients of degree 3 such that if $x = p/q$, $p' = F(p, q)$ and $q' = 4qG(p, q)$, then

$$A(p, q)p' + B(p, q)q' = cq^7.$$

Reversing the roles of x and y, one finds two more homogenous forms $A'(x, y)$ and $B'(x, y)$ with integral coefficients of degree 3 such that

$$A'(p, q)p' + B'(p, q)q' = cp^7.$$

These are the equations we used in the theory of heights in lectures.